HP ProLiant BL e-Class Integrated Administrator User Guide

May 2003 (Fourth Edition)
Part Number 249070-004

© 2003 Hewlett-Packard Development Company, L.P.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

Hewlett-Packard Company shall not be liable for technical or editorial errors or omissions contained herein. The information in this document is provided "as is" without warranty of any kind and is subject to change without notice. The warranties for HP products are set forth in the express limited warranty statements accompanying such products. Nothing herein should be construed as constituting an additional warranty.

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

HP ProLiant BL e-Class Integrated Administrator User Guide

May 2003 (Fourth Edition)
Part Number 249070-004

Contents

About This Guide

Audience Assumptions ix
Important Safety Information ix
Symbols on Equipment ix
Symbols in Text xi
Related Documents xii
Getting Help xii
Technical Support xii
HP Website xiii
Authorized Reseller xiii
Reader's Comments xiii

Chapter 1

HP ProLiant BL e-Class System Software Features

ProLiant BL e-Class Integrated Administrator 1-1
Integrated Administrator Features 1-2
Overview of ProLiant BL e-Class Software Tools 1-5

Chapter 2

Getting Started

Reviewing Configuration Tools and Information 2-1
Identifying the Integrated Administrator Connectors 2-2
Determining the Integrated Administrator's Initial IP Address 2-4
Requirements for Local Client Devices 2-4
Default Values for the Integrated Administrator 2-5
Determining the IP Address using the Local Console 2-5
Setting Up the Web-Based User Interface 2-7

Additional Steps....2-11
Help....2-11

Chapter 3
Web-Based User Interface

Accessing the Web-Based User Interface....3-2
Web-Based Navigation....3-3
Top Panel....3-3
Left Panel....3-5
Deck Panel....3-6
Enclosure Tab....3-6
Enclosure Information....3-7
Network Configuration....3-13
SNMP Configuration....3-16
Virtual Buttons....3-19
System Log....3-21
Bays Tab....3-22
Bay List....3-22
Bay Information....3-26
Remote Console....3-28
Virtual Buttons....3-30
Console Log....3-31
Administration Tab....3-32
User List....3-33
Group List....3-35
Add User....3-36
Add Group....3-39
View/Modify User....3-42
View/Modify Group....3-42
Event List Tab....3-43
Interconnect Tab....3-45

Chapter 4
Command Line Interface

Accessing tbe Command Line Interface....4-2
Accessing Remotely througb the Management Connector....4-2
Accessing Locally through the Console Connector....4-2
Operating the Command Line Interface....4-3

General Commands 4-3
General Management Commands 4-4
User Account Commands 4-7
Enclosure Network Configuration Commands 4-12
Enclosure Management Commands 4-16
Server Bay Management Commands 4-20
Command Line Event Messages 4-25
Functionality Exclusive to the Command Line Interface 4-27

Chapter 5
Setting Up the System
User Permissions 5-3
Customizing the Enclosure Settings 5-4
Changing the Administrator Password 5-4
Modifying Enclosure and Rack Names 5-5
Modifying the Asset Tag Number 5-7
Modifying the Date and Time 5-8
Setting Up User Accounts 5-10
Adding a Group 5-10
Adding a User 5-14
Enabling Remote Console Sessions to Server Blades 5-18
Setting Up AlertMail 5-22
E-mail Alerts 5-22
Setting Up IP Security 5-24
Setting Up Automatic Time Configuration (NTP) 5-25
Configuring SNMP Support 5-26
Entering a Community String 5-26
Modifying the System Location 5-27
Modifying the System Contact Information 5-28
Adding Trap Targets 5-28
Removing Trap Targets 5-29

Chapter 6
Performing Common Administrative Tasks
Managing Server Blade Bays 6-2
Opening a Remote Console Session to a Server Blade 6-2
Accessing the ROM-Based Setup Utility for a Server Blade 6-4
Reviewing Activity for a Server Blade 6-6

Powering Off the Server Blade 6-7
Identifying a Server Blade Using the Unit Identification LED 6-9
Managing the Enclosure 6-11
Reviewing the Activity of the Enclosure 6-11
Identifying the Enclosure Using the Unit Identification LED 6-13
Generating an Enclosure Summary 6-14
Identifying Problem Components 6-16
Managing Users 6-22
Modifying a User's Rights to Server Blade Bays 6-22
Disabling and Deleting User Accounts 6-25

Chapter 7
Performing Advanced Functions
Replicating the Configuration of the Integrated Administrator 7-2
Administering Security Certificates 7-4
Creating a Certificate Request 7-4
Downloading a Security Certificate 7-4
Key-Based SSH Authentication 7-5
Configuring Server Blade Boot Order 7-7
Powering Off the Enclosure 7-8
Disabling Network Protocols 7-10
Upgrading the Integrated Administrator Firmware 7-11
Recovering a Lost Administrator Password 7-12
Launching Flash Disaster Recovery 7-13

Appendix A
Command Line Conventions

Appendix B
Error Messages
Warning Messages B-1
Enclosure Warning Messages B-2
Server Blade Bay Warning Messages B-3
Administration Warning Messages B-3
Error Messages B-4
Enclosure Error Messages B-4
Server Blade Bay Error Messages B-4
Administration Error Messages B-5

Appendix C
Troubleshooting

Appendix D
Event Details

Appendix E
Factory Default Settings
Enclosure E-2
Users E-2
Groups E-3
Network E-3
Protocol E-3

Appendix F
Time Zone Settings
Universal F-2
Africa F-3
Asia F-4
Europe F-6
Oceania F-7
Polar F-9
The Americas F-10

Appendix G
Open Source Availability

Index

About This Guide

This guide provides step-by-step instructions for operation, and reference information for advanced operation, troubleshooting, and future upgrades for the HP ProLiant BL e-Class Integrated Administrator.

Audience Assumptions

This guide is intended for users with access to the ProLiant BL e-Class Integrated Administrator. It assumes that the server blade system hardware is installed, and that the user has minimal experience working with server blade systems.

⚠ Important Safety Information

Before installing this product, read the *Important Safety Information* document included with the server.

Symbols on Equipment

The following symbols may be placed on equipment to indicate the presence of potentially hazardous conditions:

WARNING: This symbol, in conjunction with any of the following symbols, indicates the presence of a potential hazard. The potential for injury exists if warnings are not observed. Consult the documentation for specific details.

This symbol indicates the presence of hazardous energy circuits or electric shock hazards. Refer all servicing to qualified personnel.

WARNING: To reduce the risk of injury from electric shock hazards, do not open this enclosure. Refer all maintenance, upgrades, and servicing to qualified personnel.

This symbol indicates the presence of electric shock hazards. The area contains no user or field serviceable parts. Do not open for any reason.

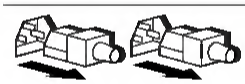
WARNING: To reduce the risk of injury from electric shock hazards, do not open this enclosure.

This symbol on an RJ-45 receptacle indicates a network interface connection.

WARNING: To reduce the risk of electric shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

This symbol indicates the presence of a hot surface or hot component. If this surface is contacted, the potential for injury exists.

WARNING: To reduce the risk of injury from a hot component, allow the surface to cool before touching.



These symbols, on power supplies or systems, indicate that the equipment is supplied by multiple sources of power.

WARNING: To reduce the risk of injury from electric shock, remove all power cords to completely disconnect power from the system.

This symbol indicates that the component exceeds the recommended weight for one individual to handle safely.

Weight in kg
Weight in lb

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manual material handling.

Symbols in Text

These symbols may be found in the text of this guide. They have the following meanings.

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or loss of life.

CAUTION: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

IMPORTANT: Text set off in this manner presents essential information to explain a concept or complete a task.

NOTE: Text set off in this manner presents additional information to emphasize or supplement important points of the main text.

Related Documents

For additional information on the topics covered in this guide, refer to the following documentation:

- *HP ProLiant BL e-Class System Maintenance and Service Guide*
- *HP ProLiant BL e-Class System Hardware Installation and Configuration* poster
- *ProLiant Integration Module for Altiris eXpress User Guide*
- *HP Servers Troubleshooting Guide*
- *HP ROM-Based Setup Utility Guide*
- *HP ProLiant BL e-Class C-GbE Interconnect Switch User Guide*
- White paper: *HP ProLiant BL e-Class System Overview and Planning*
- White paper: *Configuring a Preboot eXecution Environment (PXE) using Red Hat Linux 7.2 on ProLiant Servers*
- QuickSpecs

Getting Help

If you have a problem and have exhausted the information in this guide, you can get further information and other help in the following locations.

Technical Support

In North America, call the HP Technical Support Phone Center at 1-800-652-6672. This service is available 24 hours a day, 7 days a week. For continuous quality improvement, calls may be recorded or monitored. Outside North America, call the nearest HP Technical Support Phone Center. Telephone numbers for worldwide Technical Support Centers are listed on the HP website, www.hp.com.

Be sure to have the following information available before you call HP:

- Technical support registration number (if applicable)
- Product serial number
- Product model name and number
- Applicable error messages
- Add-on boards or hardware
- Third-party hardware or software
- Operating system type and revision level

HP Website

The HP website has information on this product as well as the latest drivers and flash ROM images. You can access the HP website at www.hp.com.

Authorized Reseller

For the name of the nearest authorized reseller:

- In tbe United States, call 1-800-345-1518.
- In Canada, call 1-800-263-5868.
- Elsewhere, see the HP website for locations and telephone numbers.

Reader's Comments

HP welcomes your comments on this guide. Please send your comments and suggestions by e-mail to `ServerDocumentation@hp.com`.

1

HP ProLiant BL e-Class System Software Features

The HP ProLiant BL e-Class system offers an extensive set of features and optional tools to support effective server management and software deployment. This chapter describes tbe Integrated Administrator and provides a brief overview of software associated with the system.

ProLiant BL e-Class Integrated Administrator

The Integrated Administrator is a centralized management and monitoring system for the ProLiant BL e-Class enclosure and server blades. The Integrated Administrator acts as a combination terminal server and remote power controller, enabling out-of-band, secure, serial console connections to all server blades in the enclosure.

The ProLiant BL e-Class Integrated Administrator is a standard component of ProLiant BL e-Class systems. The Integrated Administrator provides enclosure health, server blade health, and remote server manageability. Integrated Administrator features are accessed from any network-based client. The lntegrated Administrator provides remote access to any authorized network client, sends alerts, and provides many other server blade management functions.

The Integrated Administrator subsystem is embedded on a module included with each interconnect tray and includes an intelligent microprocessor, secure memory, and a dedicated network interface. This design makes the lntegrated Administrator independent of the host server and its operating system.

For further information associated with the Integrated Administrator, refer to:

www.compaq.com/products/servers/proliant-bl/e-class/integrated-admin.html

Integrated Administrator Features

The Integrated Administrator provides the following functionality to deliver state-of-the-art management of the enclosure and server blades:

- Dedicated LAN network connectivity

  Each Integrated Administrator provides a dedicated network connection. The NIC can auto-select speeds between 10 Mbps and 100 Mbps. When the ProLiant BL e-Class C-GbE Interconnect Switch (option) is installed, the Integrated Administrator can be configured to route through a Gigabit uplink connector using VLANS, eliminating the need for a separate management network.

- SNMP alerts from Integrated Administrator to a management console

  The Integrated Administrator provides notification of enclosure problems. Using a management console, you can access certain server blade alerts, such as SNMP and unauthorized access alerts.

- E-mail alerts from Integrated Administrator to an e-mail account (AlertMail)

  AlertMail enables the Integrated Administrator to send system events by e-mail instead of using SNMP traps. AlertMail is completely independent from SNMP and both can be enabled at the same time. AlertMail uses standard SMTP commands to communicate with any SMTP capable mail server.

- Remote access and control

  The Integrated Administrator provides remote functionality to access the console of the host server blade, change the state of the Unit Identification LED on an enclosure and its server blades, and power up, power down, or reboot a server blade.

  The Integrated Administrator displays alerts regardless of the state of the user's host server blade and integrates with the Insight Manager 7 utility using SNMP to provide alerts and diagnostics of the system.

If a server blade does not respond, this feature enables an administrator to initiate a cold reboot to bring the server blade back online. The Integrated Administrator can be used to remotely operate a power button of a server blade.

Integrated Administrator is fully accessible by means of Microsoft® Internet Explorer and Netscape. This capability enables easy access to the features of Integrated Administrator.

The Integrated Administrator also has a command line interface (CLI) accessible using Secure Shell (encrypted) or Telnet (unencrypted) protocols, providing extensive management capability to remote network users. Local users can access the CLI by attaching a client computer (using a terminal emulator) or terminal to the Integrated Administrator's console (serial) port.

IMPORTANT: With a Telnet session, all data—including passwords—are passed as clear text.

- User administration and security

  The Integrated Administrator supports up to 25 users with customizable access rights and login names. Groups are first assigned bays, and then users are given membership to those groups. This group-centered methodology is designed to facilitate user management across server blades.

  Integrated Administrator provides strong security for remote management in distributed IT environments by using industry-standard Secure Sockets Layer (SSL) encryption of HTTP data transmitted across the network. SSL encryption (up to 128-bit) ensures that the HTTP information is secure as it travels across the network. All remote console data can be encrypted as well.

  Integrated Administrator provides secure password encryption, tracking all login attempts and maintaining a record of all login failures. Integrated Administrator also provides the following additional security features:

  — User actions logged in the Integrated Administrator System Log

  — Login legal warning

  IP Security allows an administrator to define a set of IP addresses that are the only ones allowed to connect to the services provided (SSH, HTTP, HTTPS, TELNET, SNMP). This means that an administrator can make sure only a certain set of machines have access to Integrated Administrator.

- Automatic network configuration

  The Integrated Administrator provides automatic network configuration of the IP address and host name using Dynamic Host Configuration Protocol (DHCP) and Dynamic DNS/WINS. Integrated Administrator comes with a default name and DHCP client that leases an IP address from the DHCP server on the network. For networks that do not use DHCP, the Integrated Administrator enables static IP configuration.

- Automatic time configuration (NTP)

  Automatic time configuration allows Integrated Administrator to synchronize its date and time with a server supporting the Network Time Protocol (NTP).

- Integration with the Insight Manager 7 utility

  Integrated Administrator provides full integration with the Insight Manager 7 utility under key operating environments. This integration provides:

  — Support for SNMP management

    Support for SNMP trap delivery to a Insight Manager 7 console

  — Management processor

    The Insight Manager 7 utility adds support for a new device type, the management processor. All Integrated Administrators (in ProLiant BL e-Class enclosures) on the network are discovered in the Insight Manager 7 utility as management processors. The management processors are associated with the server blades they manage.

  — Integrated Administrator hyperlinks

    The Insight Manager 7 utility provides a hyperlink on the server device page to launch and connect to Integrated Administrator.

  — Grouping of Integrated Administrator processors

    All Integrated Administrator management processors can be grouped together logically and displayed on one page in the Insight Manager 7 utility. This capability provides access to all Integrated Administrators on the network from one point in Insight Manager 7.

For more information on the Insight Manager 7 utility, refer to the ProLiant Essentials Foundation Pack documentation that ships with the system or refer to:

www.hp.com/servers/rdp

- Event Notification

  The Integrated Administrator provides real-time event notifications for an enclosure. When an event occurs, the Integrated Administrator notifies connected users by generating an icon that the user can click to view more details.

- Status Information

  The Integrated Administrator enables an enclosure administrator to update the rack name, enclosure name, asset tag, time zone, date, and time, as well as observe the status and general information for every component in the enclosure.

Overview of ProLiant BL e-Class Software Tools

ProLiant BL e-Class server blade systems also support the following tools and utilities to facilitate monitoring and management of the enclosure:

- ROM-Based Setup Utility (RBSU)

  RBSU performs a wide range of configuration activities and provides access to numerous settings, including those for system devices, operating system selection, and boot controller order. RBSU is also fully compatible with remote serial console mode using the Integrated Administrator.

- Redundant ROM support

  Each server blade has two 1-MB ROM images: one of which contains the current version of the ROM, while the second contains a backup version of the ROM. If the first ROM becomes corrupt, the system defaults to the backup version, maximizing uptime and server availability.

- Headless server operation

  ProLiant BL e-Class server blades include VGA, keyboard, mouse, and USB interfaces; however, these server blades are designed primarily for headless operation and management with no keyboard or monitor attached.

- ProLiant Essentials Rapid Deployment Pack (Option)

  The Rapid Deployment Pack features a graphical deployment console, which provides intuitive drag-and-drop events, such as scripts and images, to deploy the operating systems and applications on any combination of server blades installed in the enclosures.

  The Rapid Deployment Pack integrates two powerful products: Altiris eXpress Deployment Server and the ProLiant Integration Module that contains optimizations for ProLiant servers and enables simultaneous deployment of multiple server blades.

  With the Rapid Deployment Pack, ProLiant BL e-Class users can automatically install pre-defined configurations on newly installed server blades.

  For more information about the Rapid Deployment Pack, refer to an authorized reseller, the Rapid Deployment CD that ships with the enclosure, or go to:

  www.hp.com/servers/rdp

- Insight Manager 7

  Insight Manager 7 is an easy-to-use, intuitive software utility designed for collecting server information, including fault conditions, performance, security, remote management, and recovery services. The ProLiant BL e-Class system is fully compatible with the Insight Manager 7 utility.

- Diagnostics Utility

  The Diagnostics Utility displays information about a server blade's hardware and tests the system to ensure it is operating properly.

- Automatic Server Recovery-2 (ASR-2)

  ASR-2 is a diagnostic/recovery feature that automatically restarts the server blade in the event of a critical operating system failure.

- Enclosure Self Recovery (ESR)

  ESR, similar to ASR-2, is unique to the ProLiant BL e-Class system and is a self-monitoring reliability feature of the Integrated Administrator. If the Integrated Administrator does not boot or hangs during operation, ESR automatically resets the Integrated Administrator for an attempted self-recovery. The ProLiant BL e-Class server blades and interconnect tray are not affected by ESR.

- Health and Wellness Driver (server blade health driver) and Integrated Management Log (IML) Viewer

  The server blade health driver monitors operational data of the server blades and logs abnormal conditions. This log is accessible by utilities, including Insight Manager 7, and supports the HP Management Agents.

  The server blade health driver provides the Integrated Administrator with the thermal condition, status, operating system, and the name as defined within its operating system for each server blade.

  The IML Viewer, in conjunction with the server blade health driver, provides the monitoring and management of logged system events, critical errors, power-on messages, memory errors, and any catastrophic hardware or software errors that typically cause a system to fail.

- HP Management Agents

  The HP Management Agents enable fault, performance, and configuration management on ProLiant servers, so user can focus on their business while the agents manage the servers.

- Online ROM Flash

  Using the Smart Components for Remote ROM Flash with the Remote Deployment Utility (RDU) console application, Remote ROM Flash enables you to upgrade the firmware (BIOS) on a server blade from a remote location.

- ProLiant BL e-Class C-GbE Interconnect Switch Management System and Utilities

  The ProLiant BL e-Class Interconnect Switch Management System and Utilities provide a full suite of configuration and management interfaces and tools for the ProLiant BL e-Class C-GbE Interconnect Switch (option). Full featured Web-based and menu-driven console interfaces are provided management of the interconnect switch.

  Both interfaces can be configured to require a valid username and password for authentication. RMON and SNMP manageability are supported with an SNMP-based scripting utility and sample scripts. The interconnect switch configuration can also be saved to a TFTP server as backups and as templates for preconfiguring other switches.

The interconnect switch is compatible with industry standards and has full for support for IEEE 802.1Q VLANS.

2

Getting Started

The Integrated Administrator enables monitoring and management of all functions within an enclosure, including functions specific to the server blades housed within it. Once configured, the Integrated Administrator provides these features through both a Web-based user interface and CLI.

This chapter addresses first-time configuration of the Integrated Administrator after the enclosure is installed and powered up in a rack:

- Reviewing configuration tools and information
- Identifying tbe Integrated Administrator connectors
- Determining the Integrated Administrator initial IP address
- Setting up the Web-based user interface
- Additional steps
- Help

Reviewing Configuration Tools and Information

The ProLiant BL e-Class Integrated Administrator is ready for operation immediately after powering up. The following features and information are designed to facilitate the setup and management of the Integrated Administrator:

- Each Integrated Administrator ships with a unique preconfigured Administrator password and host name.

- If the network uses Dynamic DNS or WINS, you can access the Integrated Administrator using the factory-configured host name.

IMPORTANT: The preconfigured Administrator password and host name are displayed on the Integrated Administrator Default Network Settings Tag (settings tag) attached to the interconnect tray.

- If the network uses DHCP, an IP address can be automatically assigned to the Integrated Administrator.
- The server blade health driver enables the Integrated Administrator to gracefully power down the server blades and provides the Integrated Administrator with the name as defined within the operating system of the server blade, thermal condition, status, and operating system for each server blade.

CAUTION: Without the server blade health driver or an ACPI-compliant operating system, the Integrated Administrator cannot gracefully shut down a server blade. This condition may result in the permanent loss of critical data.

Identifying the Integrated Administrator Connectors

Each ProLiant BL e-Class interconnect tray ships with the Integrated Administrator module already installed and provides external connectivity using two connectors on the rear panel.

CAUTION: Do not plug anything into the enclosure link connectors. They are reserved for future use and are not designed to accept a 10/100 Ethernet connector.

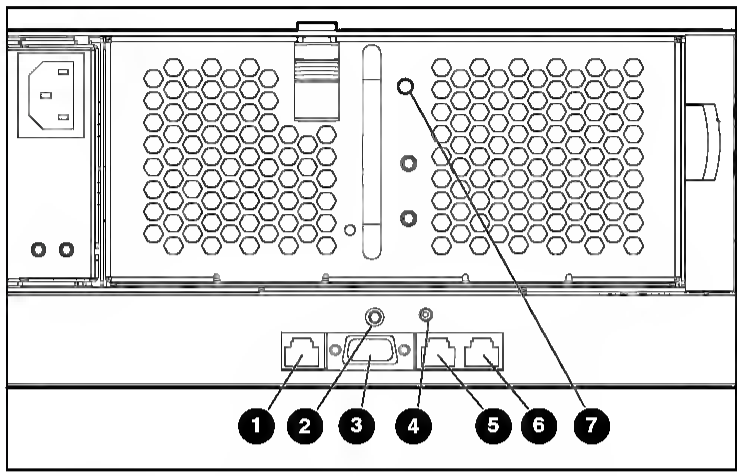


Figure 2-1: Rear panel Integrated Administrator components

Table 2-1: Rear Panel Integrated Administrator Components

Item	Description
1	Management (10/100 Ethernet) connector for remote access through a Web-based user interface, Telnet, or Secure Shell
2	Integrated Administrator reset button
3	Console (serial) connector for local access to the command line interface using a laptop computer
4	Integrated Administrator health LED
5 & 6	Enclosure link connectors (see previous Caution)
7	Enclosure Unit Identification button

Determining the Integrated Administrator's Initial IP Address

HP recommends that you connect a local client device, such as a laptop computer, to the console (serial) connector in order to determine the initial IP address used by the network to recognize the Integrated Administrator. After using that IP address to access the Integrated Administrator locally using the console (serial) connector, you can use the Integrated Administrator default values to complete the initial configuration.

The organization of this section reflects this process:

- Requirements for local client devices
- Default values for the Integrated Administrator
- Determining the IP address using the local console

Requirements for Local Client Devices

You can access the Integrated Administrator locally using the serial connector on the rear panel of the enclosure using a local client device, such as a laptop computer.

The local client device must run a terminal emulator, such as HyperTerminal for Windows systems or Kermit for Linux systems.

The terminal emulator must operate at the following settings:

- Bits per second: 9600
- Bits: 8
- Parity: None
- Stop bits: 1
- Flow control: none
- Emulation: VT100
- Backspace key sends **Ctrl-H**

Default Values for the Integrated Administrator

The Integrated Administrator is configured with a default user name, password, and DNS name. A settings tag with the preconfigured values is attached to the interconnect tray containing the Integrated Administrator module.

IMPORTANT: For security reasons, HP recommends changing the Administrator password when accessing Integrated Administrator for the first time.

Determining the IP Address using the Local Console

To determine the Integrated Administrator IP address using the local console:

1. Access the Integrated Administrator console:
   a. Connect a local client device (such as a laptop computer) with VT100 terminal emulation software to the Integrated Administrator (serial) console connector using the null-modem serial cable (provided with the enclosure).

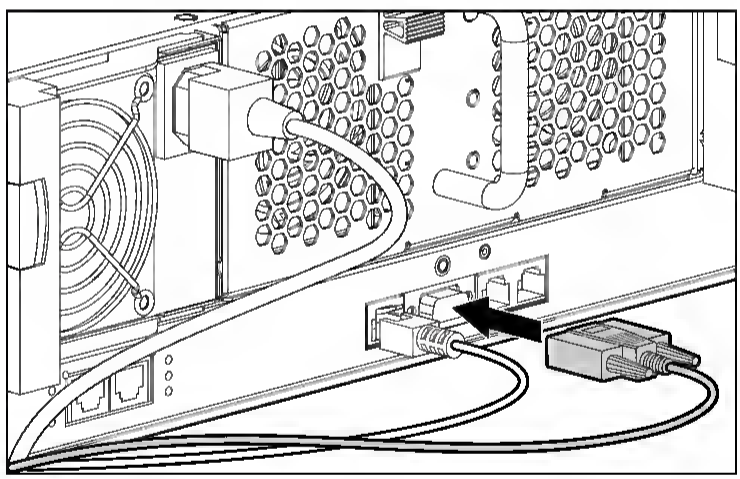


Figure 2-2: Installing a local client device to the Integrated Administrator (serial) console connector

b. Open a terminal emulation session with the following settings: 9600 bps, 8 data bits, no parity, and 1 stop bit.

c. Log into the Integrated Administrator using the password on the settings tag attached to the interconnect tray.

2. Establish the Integrated Administrator IP address.

   For a detailed explanation of the command line conventions used in this document, see Appendix A, "Command Line Conventions."

   — If a DHCP server is attached to the network, determine the Integrated Administrator IP address. Enter the following command at the command line interface:

   ```
   SHOW NETWORK
   ```

   — If a DHCP server is not attached to the network, enter the following commands sequentially to assign a static IP address to the Integrated Administrator:

   ```
   SET IPCONFIG STATIC <IP address> <subnet mask>
   SET GATEWAY <IP address>
   SET DNS <primary address> {<secondary address>}
   ```

   You can now access the Integrated Administrator using a web browser, Secure Shell, Telnet, or SNMP.

Setting Up the Web-Based User Interface

To set up the Web-based user interface:

1. Enter the Integrated Administrator IP address or DNS name in the address bar of the Web browser.

   A security alert appears as an expected part of this procedure.

Security Alert
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate
The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority
The security certificate date is valid
The name on the security certificate is invalid or does not match the name of the site
Do you want to proceed?
Yes
No
View Certificate

Figure 2-3: Certificate Security Alert

— If you click **Yes,** the browser continues to the **Login** window of Integrated Administrator. The alert message appears each time you access the Integrated Administrator management processor in a browser.

— If you click **No,** you are returned to what was previously displayed on your browser.

— If you click **View Certificate,** a popup window displays the certificate information, as shown in Figure 2-4. Installing the certificate to your browser prevents the security alert message from displaying in the future.

NOTE: To install your own certificate onto the Integrated Administrator rather than the automatically generated certificate, see the information on certificate-related commands in Table 4-8 as well as the "Administering Security Certificates" section in Chapter 7, "Performing Advanced Functions."

Figure 2-4: Certificate Information window

IMPORTANT: If the certificate is removed from your browser, the security alert message is displayed again.

2. Install the certificate to your browser:
   a. Click **Install Certificate.** The Certificate Manager Import Wizard starts.
   b. Click **Next.**
   c. Click **Next** for the browser to automatically select the certificate store when the **Certificate Store** window appears.
   d. Click **Finish** when the **Completing the Certificate Manager Import Manager Wizard** window displays.
   e. Click **Yes** to confirm the installation of the certificate when the confirmation window displays.
3. The screen prompts you for a user name and password. Use the default user name and password from the settings tag attached to the interconnect tray and click **Log In.**

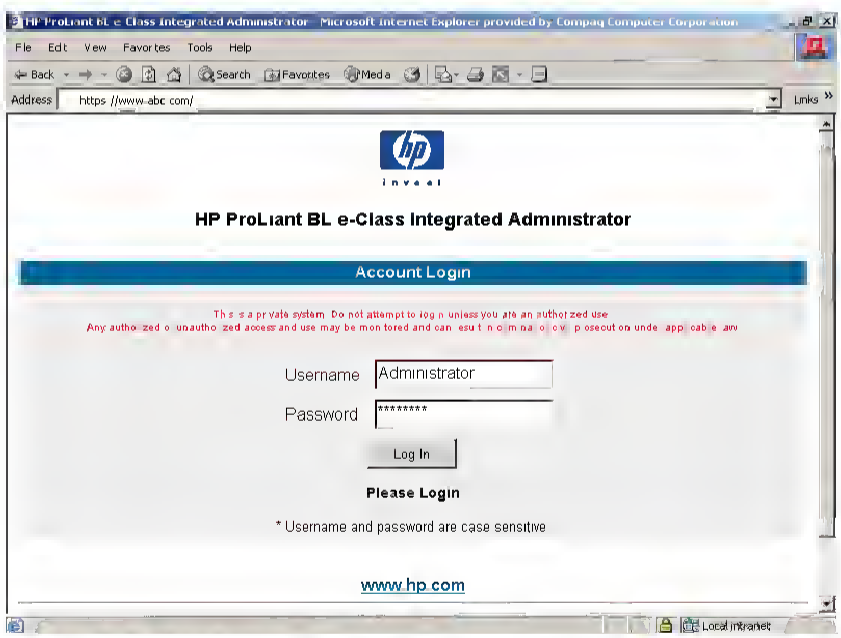


Figure 2-5: Login screen

After the default user name and password have been verified, the summary window appears.

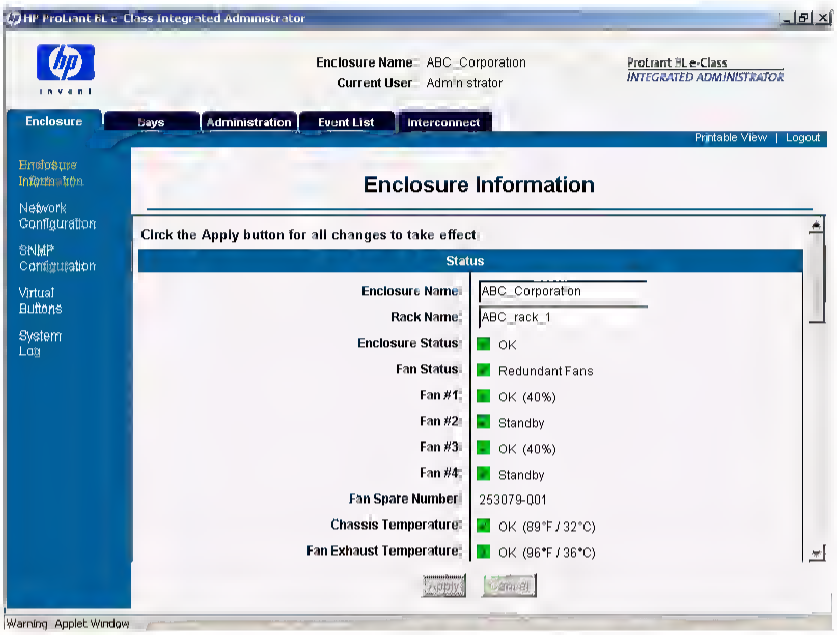


Figure 2-6: Integrated Administrator summary window

The Integrated Administrator summary window provides general information about the Integrated Administrator, such as the user currently logged on, enclosure name and status, and Integrated Administrator IP address and name.

Additional Steps

HP recommends performing the following tasks:

- Change the Administrator password
- Set the date and time
- Name the enclosure and rack
- Set up groups, users, and access privileges

For detailed instructions on performing these tasks, see the appropriate sections in Chapter 5, "Setting Up the System."

Help

Additional assistance is available by means of the Integrated Administrator help option. These links provide summary information about the features of Integrated Administrator and helpful information for optimizing the operation of Integrated Administrator.

3

Web-Based User Interface

This chapter provides information for navigating the Integrated Administrator Web-based user interface.

NOTE: Values appearing in the screens of this chapter are for illustrative purposes only.

Accessing the Web-Based User Interface

IMPORTANT: Accessing the Web-based user interface is not supported from the console (serial) connector.

To access the Integrated Administrator Web-based user interface with HTTP:

1. Get the DNS name from the settings tag attached to the interconnect tray.
2. Open a Web browser and enter the IP address or DNS name for the enclosure you wish to access.

CAUTION: If your network does not provide DHCP and either Dynamic DNS or WINS services, you need to configure a static IP address. See the "Accessing the Command Line Interface Locally" section in Chapter 4, "Command Line Interface."

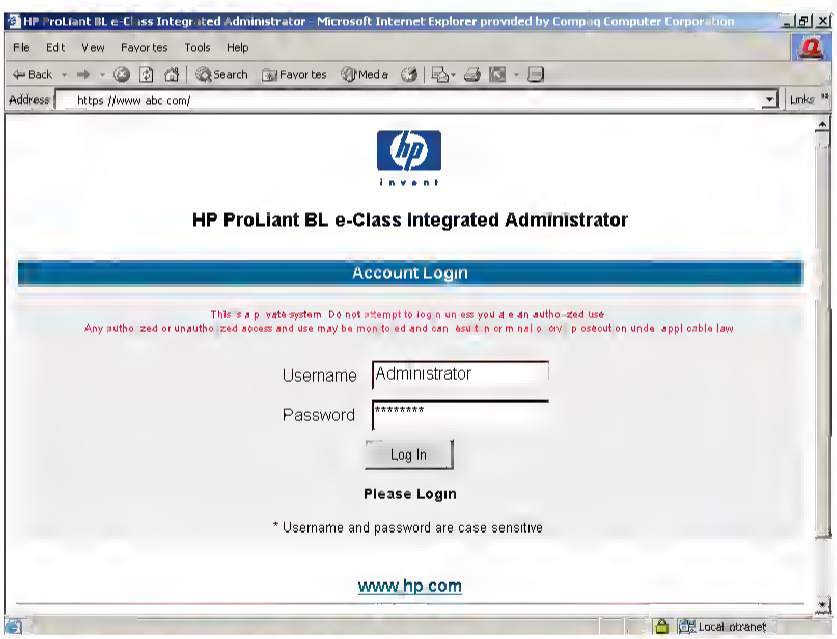


Figure 3-1: Viewing the Login screen

3. Enter the user name and password at the Login prompt.

Web-Based Navigation

The Web-based user interface displays information and receives input in the following areas:

- Top panel
- Left panel
- Deck panel

Top Panel

Figure 3-2 illustrates the location of the top panel.

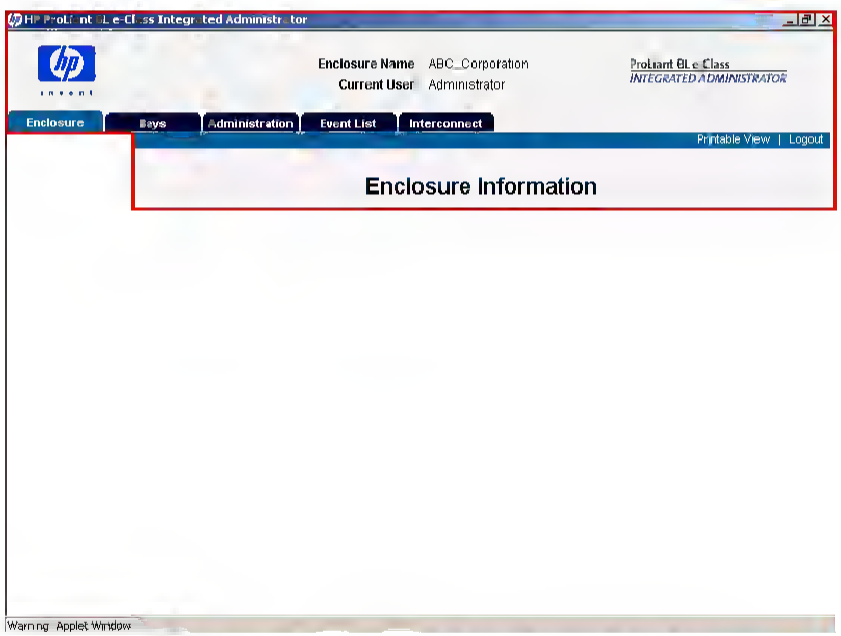


Figure 3-2: Top panel of the Web-based user interface

The top panel information is displayed at all times, including the following items:

- Enclosure name
- Current user
- Tabs

The Integrated Administrator top panel provides real-time event notifications for an enclosure according to two categories: caution and critical. When an event occurs, the Integrated Administrator notifies the user by generating an icon that the user can click to view more details:

Table 3-1: Event Notification Symbols

Icon	Description
	Caution
	Critical

For a comprehensive list of events that trigger real-time notifications in a format that reflects the Integrated Administrator representation, see Appendix D, "Event Details."

Two buttons appear on the top panel:

- **Printable View** — Opens a separate window that shows information for cutting and pasting purposes
- **Log Out** — Logs you out of the Web-based user interface

Left Panel

Figure 3-3 illustrates the location of the left panel.

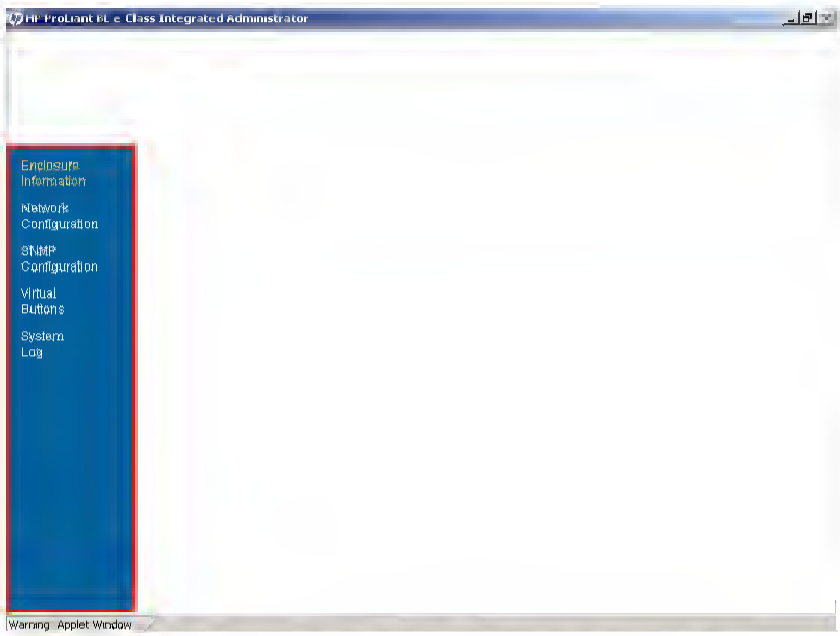


Figure 3-3: Left panel of the Web-based user interface

The left panel displays which screens are available under each tab. Information appearing in the left panel depends on which tab the user chooses from within the top panel.

Deck Panel

Figure 3-4 illustrates the location of the deck panel.

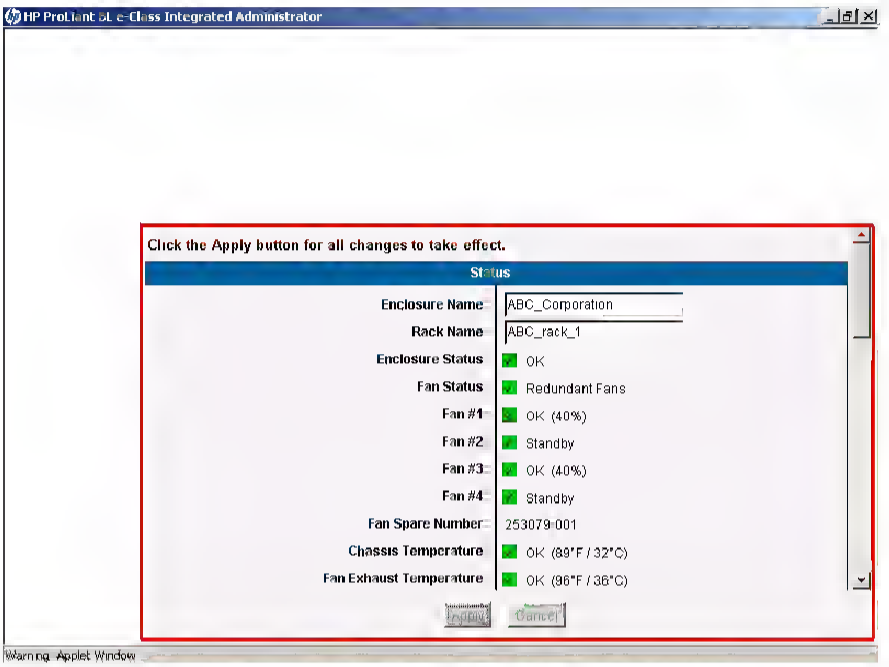


Figure 3-4: Deck panel of the Web-based user interface

The deck panel displays the areas of information provided by the available screens under each tab. Information appearing in the deck panel depends on the option chosen by the user from within the top panel and the left panel.

Enclosure Tab

The **Enclosure** tab provides access to the following screens:

- Enclosure Information
- Network Configuration
- SNMP Configuration

- Virtual Buttons
- System Log

Enclosure Information

IMPORTANT: All users have read access to the information in this screen.

Figure 3-5 illustrates the information presented on the **Enclosure Information** screen.

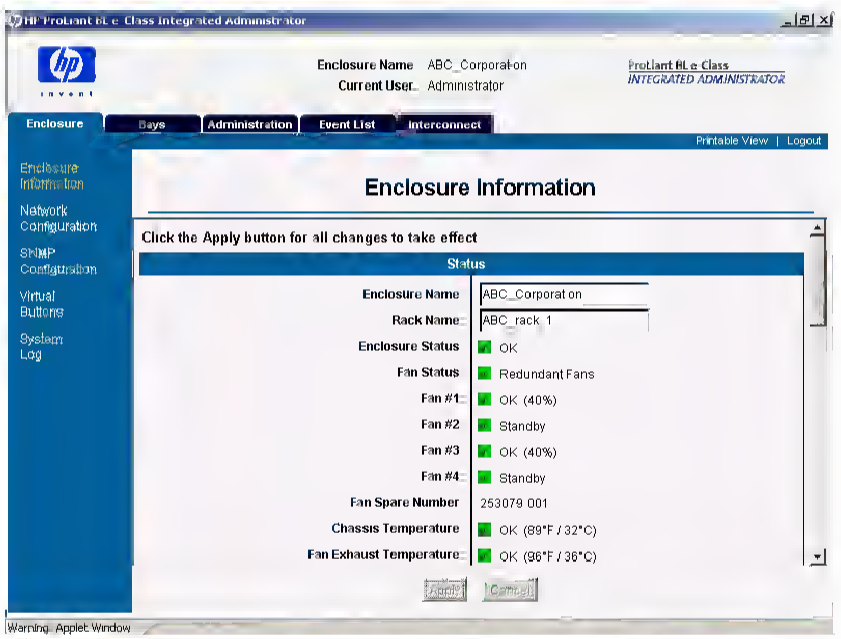


Figure 3-5: Enclosure Information screen (status area, 1 of 6, shown)

The **Enclosure Information** screen enables an enclosure administrator to update the rack name, enclosure name, asset tag, time zone, date, and time, as well as observe the status and general information for every component in the enclosure.

Two buttons appear on the **Enclosure Information** screen:

- **Apply** — Saves changes made to the screen
- **Cancel** — Restores all fields on the screen to their original values

Table 3-2 describes the information displayed in the areas that comprise the **Enclosure Information** screen.

Table 3-2: Enclosure Information Screen

Field	Possible Values	Description
Status Area		
Enclosure Name	Maximum 32 characters including all alphanumeric, dash, and underscore characters	Name of the enclosure Only enclosure administrators have write access to this field. For the default enclosure name, see Appendix E, "Factory Default Settings."
Rack Name	Maximum 32 characters including all alphanumeric, dash, and underscore characters	Name of the rack Only enclosure administrators have write access to this field. For the default rack name, see Appendix E, "Factory Default Settings."
Enclosure Status	OK, Degraded, or Failed	Status of the enclosure
Fan Status	Redundant or Non-redundant	Redundant: all fans are functional. Non-redundant: at least one fan is not functional.
Fan #1 – Fan #4	OK, Standby, Degraded, Failed, or Testing Percentage of full fan speed	Status of fans 1 through 4
Fan Spare Number		The spare number for the fans installed in the enclosure

continued

Table 3-2: Enclosure Information Screen *continued*

Field	Possible Values	Description
Temperature	OK, Warm, Caution, or Critical	Enclosure component temperature sensor
Power Area		
Power Subsystem Status	Redundant or Non-redundant	Redundant: both power supplies are functional. Non-redundant: one power supply is missing or not functional.
Total Capacity	Watts	Total capacity of the power supplies
Power Supply #1 and #2 Status	OK, Degraded, or Failed	Status of power supply #1 and power supply #2
AC Input #1 and #2 Status	OK, Degraded, or Failed	Status of AC input to power supply #1 and AC input to power supply #2
Power Supply Spare Number		The spare number for the power supplies installed in the enclosure
General Area		
Enclosure Type		Enclosure product type
Option Part Number		Part number for the enclosure
Serial Number		Serial number for the enclosure
Asset Tag	Maximum 31 characters including all alphanumeric, dash, and underscore characters	Asset tag Only enclosure administrators have write access to this field. For the default asset tag value, see Appendix E, "Factory Default Settings."

continued

Table 3-2: Enclosure Information Screen *continued*

Field	Possible Values	Description
General Area, continued		
Interconnect Tray Type	ProLiant BL e-Class C-GbE Interconnect Switch ProLiant BL e-Class RJ-21 Interconnect ProLiant BL e-Class RJ-45 Interconnect	Type of interconnect tray
Interconnect Tray Part Number		Part number for the interconnect tray
Interconnect Tray Spare Number		Spare number for the interconnect tray
Interconnect Tray Serial Number		Serial number for the interconnect tray
Integrated Administrator Area		
Hardware Version		Hardware version of the Integrated Administrator of the enclosure
Software Version		Software version of the Integrated Administrator of the enclosure
Network Area		
IP Address	###.###.###.###, where ### ranges from 0 to 255	The IP address of the Integrated Administrator
DHCP	Enabled or Disabled	Shows the status of DHCP
Dynamic DNS	Enabled or Disabled	Shows the status of Dynamic DNS This field only appears if DHCP is enabled.
MAC Address	##:##:##:##:##:##, where ## ranges from 00 to FF	The MAC address of the Integrated Administrator

continued

Table 3-2: Enclosure Information Screen *continued*

Field	Possible Values	Description
Date and Time Area*		
Time Zone	Drop-down box with standard time zones listed	Time zone assigned to the enclosure For the default time zone, see Appendix E, "Factory Default Settings." For a list of all supported time zones, see Appendix F, "Time Zone Settings." For a detailed description of how to set the time zone of the enclosure to a value not listed in the drop-down box, select option **Other** and see Figure 3-6.
Date	mm/dd/yyyy	The date assigned to the enclosure
Time	hh:mm (24-hour time)	The time assigned to the enclosure

* This section of the screen is not available on Linux browsers. If you are using a Linux system, use the command line interface to change the date, time, and time zone.

IMPORTANT: Only enclosure administrators have access to the Date and Time information. If those fields are not being modified, the Integrated Administrator updates these fields every 20 seconds. If automatic time configuration is enabled, the date and time fields are grayed out and cannot be modified.

If you select **Other** for time zone, use the following window to set a user-defined time zone:

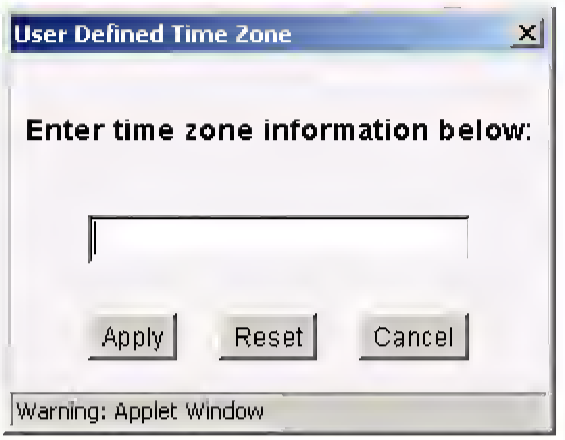


Figure 3-6: User-defined time zone window

Three buttons appear on this window:

- **Apply** — Applies the new time zone
- **Reset** — Clears the time zone text box
- **Cancel** — Cancels all changes and closes the window

For more information on accepted time zones, refer to Appendix F, "Time Zone Settings".

Network Configuration

IMPORTANT: Only enclosure administrators have access to these settings.

Figure 3-7 illustrates the information presented on the **Network Configuration** screen.

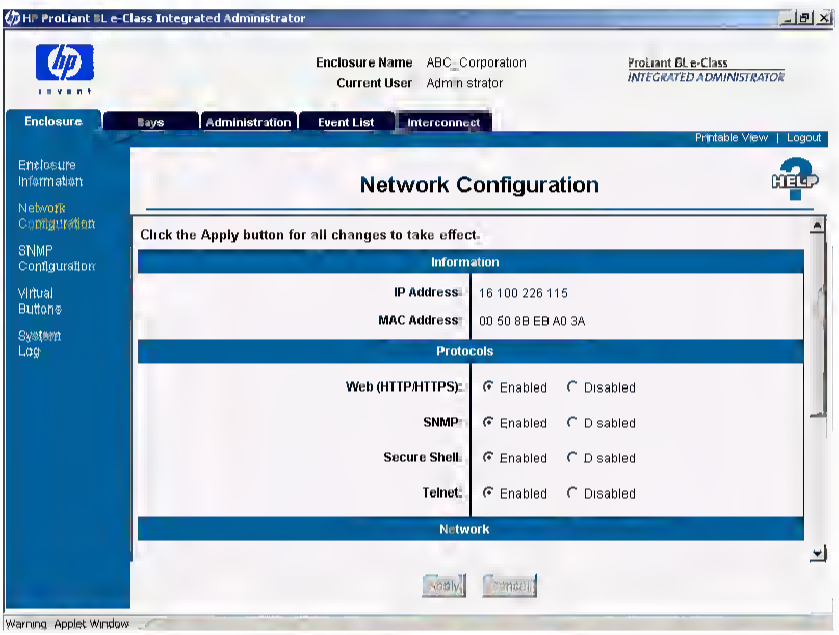


Figure 3-7: Network Configuration screen (information and protocols areas, 1 and 2 of 3, shown)

The **Network Configuration** screen enables the enclosure administrator to modify the network settings of an enclosure. These settings are specific to the enclosure and do not affect the network configurations for server blades.

Two buttons appear at the bottom of this screen:

- **Apply** — Saves changes made to the screen
- **Cancel** — Restores all fields on the screen to their original values

CAUTION: Both the Web and Secure Shell protocols must be enabled to allow access to the Web-based user interface.

Table 3-3 describes the information displayed in the areas that comprise the **Network Configuration** screen.

Table 3-3: Network Configuration Screen

Field	Possible Values	Description
Information Area		
IP Address		The IP address of the Integrated Administrator
MAC Address		The MAC address of the Integrated Administrator
Protocols Area		
Web (HTTP/HTTPS)	Enabled or Disabled	The default setting for each of the protocol radio buttons is **Enabled**. For more information on the default settings of the system , see Appendix E, "Factory Default Settings."
SNMP	Enabled or Disabled	
Secure Shell	Enabled or Disabled	
Telnet	Enabled or Disabled	
Network Area		
DHCP		Gets the IP address of the Integrated Administrator from a DHCP server
Static IP		Sets a static IP address of the Integrated Administrator
Dynamic DNS		Determines whether the Integrated Administrator uses Dynamic DNS
IP Address	###.###.###.###, where ### ranges from 0 to 255	Static IP address for the Integrated Administrator (mandatory if Static IP is selected)

continued

Table 3-3: Network Configuration Screen *continued*

Field	Possible Values	Description
Network Area, continued		
Subnet Mask	###.###.###.###, where ### ranges from 0 to 255	Subnet mask for the Integrated Administrator (mandatory if Static IP is selected)
Gateway Address	###.###.###.###, where ### ranges from 0 to 255	Gateway address for the Integrated Administrator (optional field if Static IP is selected)
DNS Server 1	###.###.###.###, where ### ranges from 0 to 255	The IP address for the primary DNS server (optional field if Static IP is selected)
DNS Server 2	###.###.###.###, where ### ranges from 0 to 255	The IP address for the secondary DNS server (optional field if Static IP is selected)

SNMP Configuration

IMPORTANT: Only enclosure administrators have access to these settings.

Figure 3-8 illustrates the information presented on the **SNMP Configuration** screen.

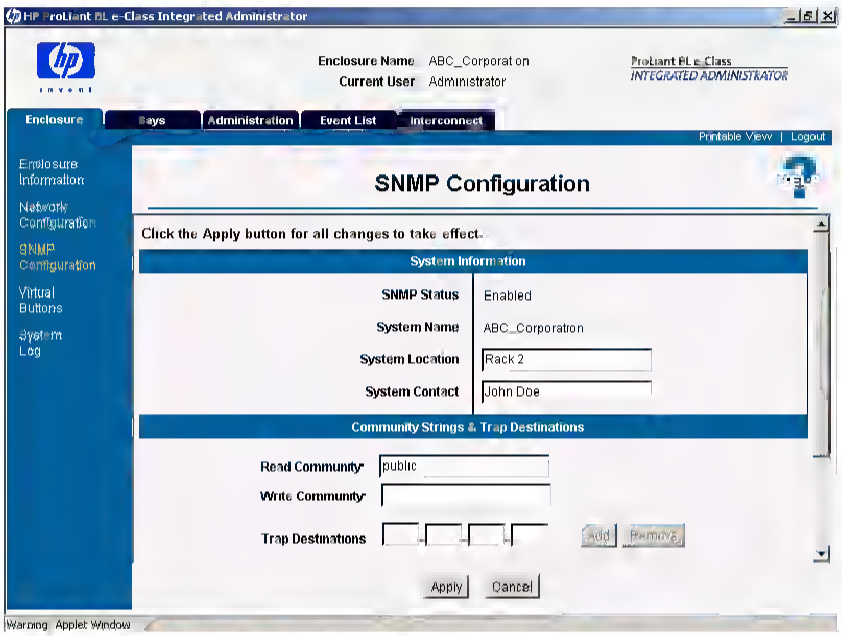


Figure 3-8: SNMP Configuration screen

The **SNMP Configuration** screen enables an enclosure administrator to modify the SNMP settings of an enclosure. These settings are specific to the enclosure and do not affect the network configurations for server blades.

Two buttons appear at the bottom of this screen:

- **Apply** — Saves changes made to the screen
- **Cancel** — Restores all fields on the screen to their original values

Table 3-4 describes the information presented on the **SNMP Configuration** screen:

Table 3-4: SNMP Configuration Screen

Field	Possible Values	Description
System Information Area		
SNMP Status	Enabled or Disabled	Displays if SNMP is enabled or disabled
System Name		The name of the enclosure
System Location	Up to 20 characters including all alphanumeric, dash, underscore, and space characters	The SNMP location of the enclosure For the default SNMP location, see Appendix E, "Factory Default Settings."
System Contact	Up to 20 characters including all alphanumeric, dash, underscore, and space characters	The SNMP contact of the enclosure For the default SNMP contact, see Appendix E, "Factory Default Settings."
Community Strings And Trap Destinations Area		
Read Community	1-20 characters including all alphanumeric, dash, and underscore characters	Displays the SNMP read community string If this is left blank, "public" is assigned. For the default Read community string, see Appendix E, "Factory Default Settings."

continued

Table 3-4: SNMP Configuration Screen *continued*

Field	Possible Values	Description
Community Strings And Trap Destinations Area, continued		
Write Community	Up to 20 characters including all alphanumeric, dash, and underscore characters	Sets the SNMP write community string If this is left blank, SNMP SET commands are disabled. For the default Read community string, see Appendix E, "Factory Default Settings."
Add		Adds an IP address to the list of trap destinations
Remove		Removes the selected IP addresses from the list of trap destinations

Virtual Buttons

IMPORTANT: Only enclosure administrators can execute these commands.

Figure 3-9 illustrates the information presented on the **Virtual Buttons** screen.

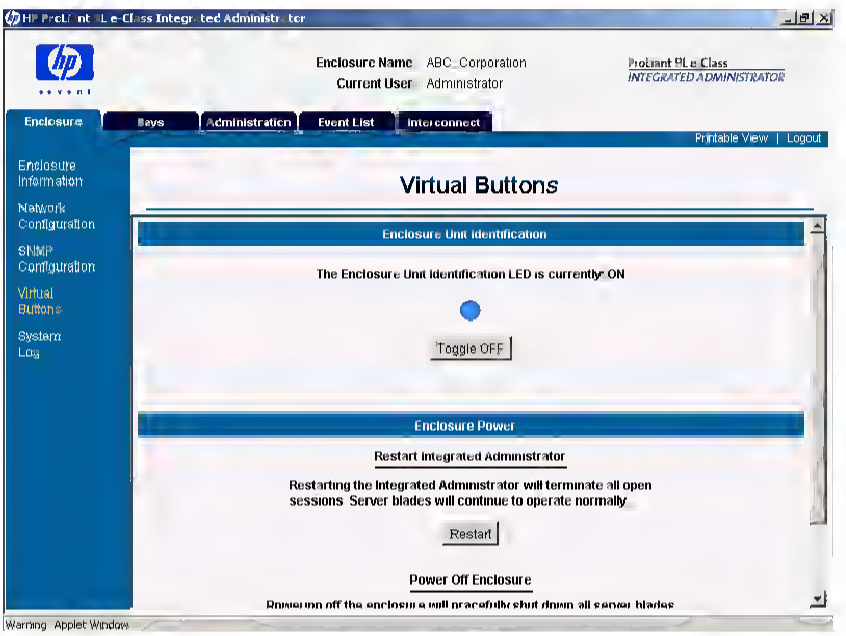


Figure 3-9: Virtual Buttons screen (Enclosure tab)

The **Virtual Buttons** screen enables an enclosure administrator to modify the power state of the enclosure and Unit Identification LED from a remote location in order to facilitate troubleshooting by technicians in the data center.

The **Toggle On/Toggle Off** button remotely changes the state of the enclosure Unit Identification LED.

Figure 3-10 describes the information presented in the Enclosure Power area of the **Virtual Buttons** screen:

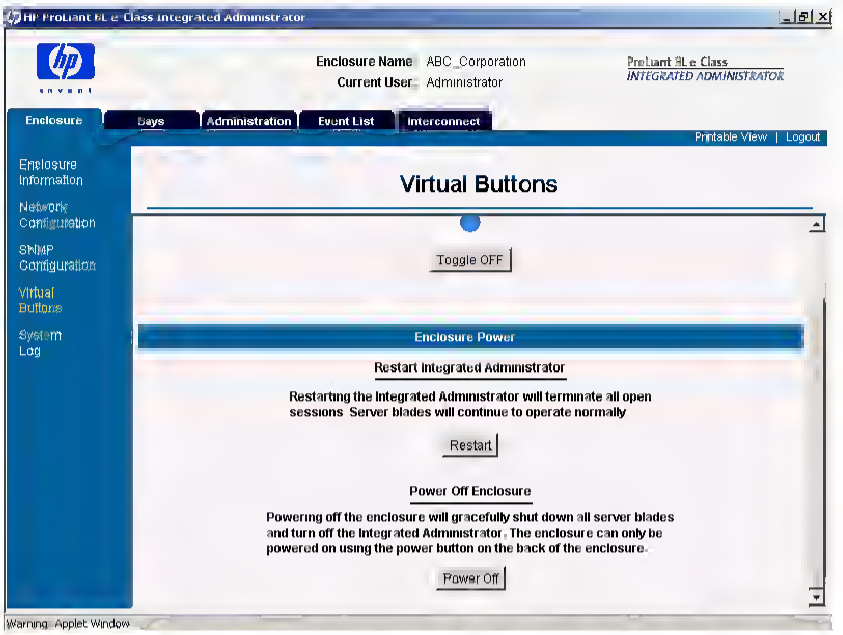

Enclosure Name ABC_Corporation
Current User Administrator
ProLiant BLe Class
INTEGRATED ADMINISTRATOR
Enclosure
Bays
Administration
Event List
Interconnect
Printable View | Logout
Enclosure Information
Network Configuration
SNMP Configuration
Virtual Buttons
System Log
Virtual Buttons
Toggle OFF
Enclosure Power
Restart Integrated Administrator
Restarting the Integrated Administrator will terminate all open sessions. Server blades will continue to operate normally.
Restart
Power Off Enclosure
Powering off the enclosure will gracefully shut down all server blades and turn off the Integrated Administrator. The enclosure can only be powered on using the power button on the back of the enclosure.
Power Off
Warning: Applet Window

Figure 3-10: Virtual Buttons screen (Enclosure Power area)

You can select the appropriate function with the following buttons:

- **Restart Integrated Administrator** restarts the Integrated Administrator and does not affect the server blades.

  IMPORTANT: Click **Restart Integrated Administrator** only at the direction of HP support personnel. You must click **Apply** for these settings to take effect.

- **Power Off Enclosure** attempts a graceful shutdown of the system for 5 minutes, after which time this command powers down all components of the enclosure immediately.

  IMPORTANT: Whenever possible, HP recommends that you use the operating system shutdown procedures before powering down a server blade or enclosure. After the enclosure is powered off, powering on can only occur by local access to the system.

System Log

The **System Log** screen provides an enclosure administrator with a chronological list of events and fixes associated with the enclosure.

Two buttons appear at the bottom of this screen:

- **Refresh** — Refreshes the screen
- **Clear** — Clears the system log

Figure 3-11 describes the information presented in the **System Log** screen:

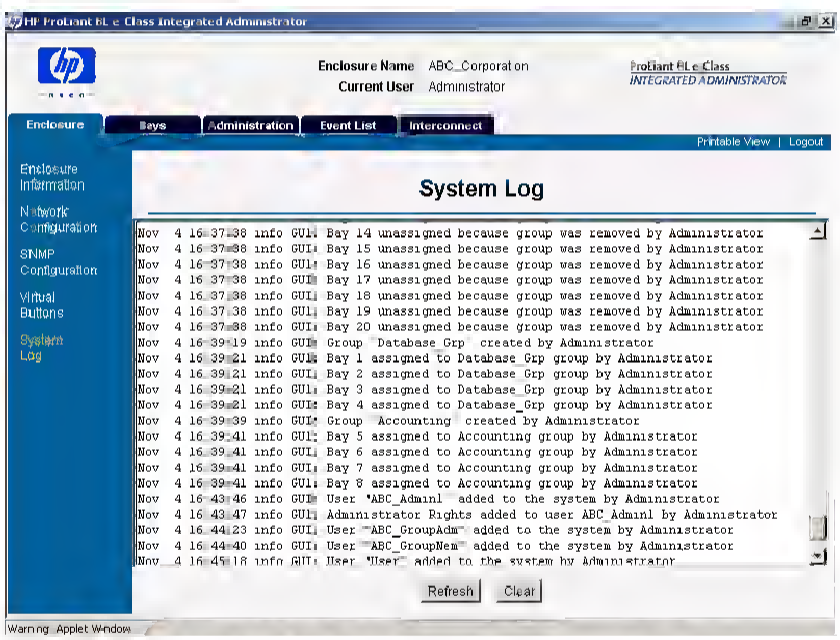

HP ProLiant BL e-Class Integrated Administrator
Enclosure Name ABC_Corporation
Current User Administrator
ProLiant BL e-Class
INTEGRATED ADMINISTRATOR
Enclosure
Bays
Administration
Event List
Interconnect
Printable View | Logout
Enclosure Information
Network Configuration
SNMP Configuration
Virtual Buttons
System Log
System Log
Nov 4 16:37:38 info GUI: Bay 14 unassigned because group was removed by Administrator
Nov 4 16:37:38 info GUI: Bay 15 unassigned because group was removed by Administrator
Nov 4 16:37:38 info GUI: Bay 16 unassigned because group was removed by Administrator
Nov 4 16:37:38 info GUI: Bay 17 unassigned because group was removed by Administrator
Nov 4 16:37:38 info GUI: Bay 18 unassigned because group was removed by Administrator
Nov 4 16:37:38 info GUI: Bay 19 unassigned because group was removed by Administrator
Nov 4 16:37:38 info GUI: Bay 20 unassigned because group was removed by Administrator
Nov 4 16:39:19 info GUI: Group "Database_Grp" created by Administrator
Nov 4 16:39:21 info GUI: Bay 1 assigned to Database_Grp group by Administrator
Nov 4 16:39:21 info GUI: Bay 2 assigned to Database_Grp group by Administrator
Nov 4 16:39:21 info GUI: Bay 3 assigned to Database_Grp group by Administrator
Nov 4 16:39:21 info GUI: Bay 4 assigned to Database_Grp group by Administrator
Nov 4 16:39:39 info GUI: Group "Accounting" created by Administrator
Nov 4 16:39:41 info GUI: Bay 5 assigned to Accounting group by Administrator
Nov 4 16:39:41 info GUI: Bay 6 assigned to Accounting group by Administrator
Nov 4 16:39:41 info GUI: Bay 7 assigned to Accounting group by Administrator
Nov 4 16:39:41 info GUI: Bay 8 assigned to Accounting group by Administrator
Nov 4 16:43:46 info GUI: User "ABC_Admin1" added to the system by Administrator
Nov 4 16:43:47 info GUI: Administrator Rights added to user ABC_Admin1 by Administrator
Nov 4 16:44:23 info GUI: User "ABC_GroupAdm" added to the system by Administrator
Nov 4 16:44:40 info GUI: User "ABC_GroupNem" added to the system by Administrator
Nov 4 16:45:18 info GUI: User "User" added to the system by Administrator
Refresh
Clear
Warning: Applet Window

Figure 3-11: System Log screen

Bays Tab

The **Bays** tab provides access to the following screens:

- Bay List
- Bay Information
- Remote Console
- Virtual Buttons
- Console Log

Bay List

The **Bay List** screen enables an enclosure administrator to observe and update the assignment of groups to server blade bays, as well as monitor the status of each server blade installed in the enclosure.

Group administrators and group members with permissions can view the server blade bays assigned to their groups.

Figure 3-12 and Table 3-5 describe the information presented in the **Bay List** screen:

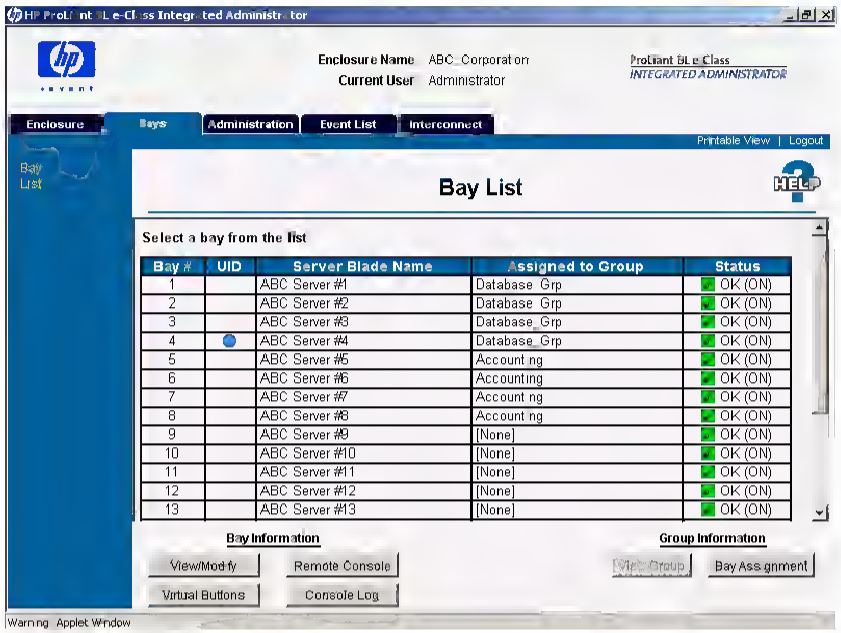

Enclosure Name ABC_Corporation
Current User Administrator
ProLiant BL e-Class
INTEGRATED ADMINISTRATOR
Enclosure
Bays
Administration
Event List
Interconnect
Printable View | Logout
Bay List
Bay List
HELP
Select a bay from the list
Bay # | UID | Server Blade Name | Assigned to Group | Status
1 | ABC Server #1 | Database_Grp | OK (ON)
2 | ABC Server #2 | Database_Grp | OK (ON)
3 | ABC Server #3 | Database_Grp | OK (ON)
4 | ABC Server #4 | Database_Grp | OK (ON)
5 | ABC Server #5 | Accounting | OK (ON)
6 | ABC Server #6 | Accounting | OK (ON)
7 | ABC Server #7 | Accounting | OK (ON)
8 | ABC Server #8 | Accounting | OK (ON)
9 | ABC Server #9 | [None] | OK (ON)
10 | ABC Server #10 | [None] | OK (ON)
11 | ABC Server #11 | [None] | OK (ON)
12 | ABC Server #12 | [None] | OK (ON)
13 | ABC Server #13 | [None] | OK (ON)
Bay Information
Group Information
View/Modify
Remote Console
Virtual Buttons
Console Log
Bay Assignment
Warning: Applet Window

Figure 3-12: Bay List screen

Table 3-5: Bay List Field Descriptions

Field	Possible Values	Description
Bay #	1-20	Server blade bay number
UID Field		Displays a blue circle if the unit identification (UID) LED of the blade is lit
Server Blade Name		Name of the server blade in that server blade bay as defined by the operating system of the server blade **Note:** Without the server blade health driver properly installed, the Integrated Administrator cannot obtain the server blade name.
Assigned to Group		Name of the group that owns that bay
Status	OK, Degraded, or Failed	The status and power state of the server blade

Please note the following permissions related to the action buttons of the **Bay List** screen (Table 3-6).

Table 3-6: Bay List Action Buttons and Permissions

Button	Function	Permissions
View/Modify	Opens the **Blade Information** screen	Enclosure administrators, group administrators, and group members with permissions
Remote Console	Opens the **Remote Console** screen	Enclosure administrators and group administrators with permissions
Virtual Buttons	Opens the **Virtual Buttons** screen	Enclosure administrators and group administrators with permissions
Console Log	Opens the **Console Log** screen	Enclosure administrators, group administrators, and group members with permissions
View Group	Opens the **View/Modify Group** screen	Enclosure administrators only
Bay Assignment	Opens the **Bay Assignment** dialog box (see Figure 3-12)	Enclosure administrators only

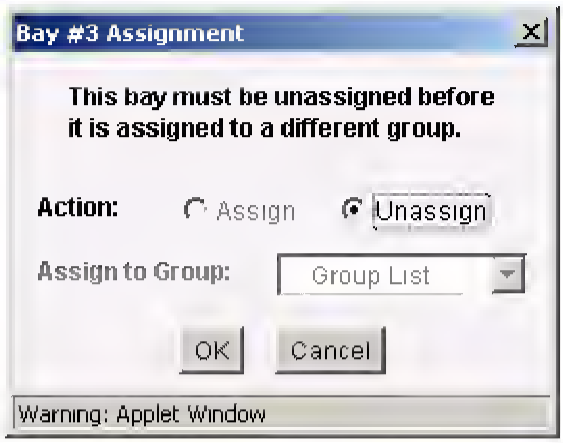


Figure 3-13: Bay Assignment dialog box

The **Action** radio buttons (Assign/Unassign) determine what action to take when you click **OK**.

IMPORTANT: If you wish to reassign a server blade from one group to another, you must first unassign the server blade; otherwise the command does not execute.

The **Assign to Group** drop-down box contains all groups within the enclosure to determine the group with ownership of the server blade bay.

Bay Information

IMPORTANT: Be sure the Integrated Administrator displays up-to-date server blade information by rebooting the server blade after installing the server blade health driver.

Figure 3-14 illustrates the information presented on the **Bay Information** screen.

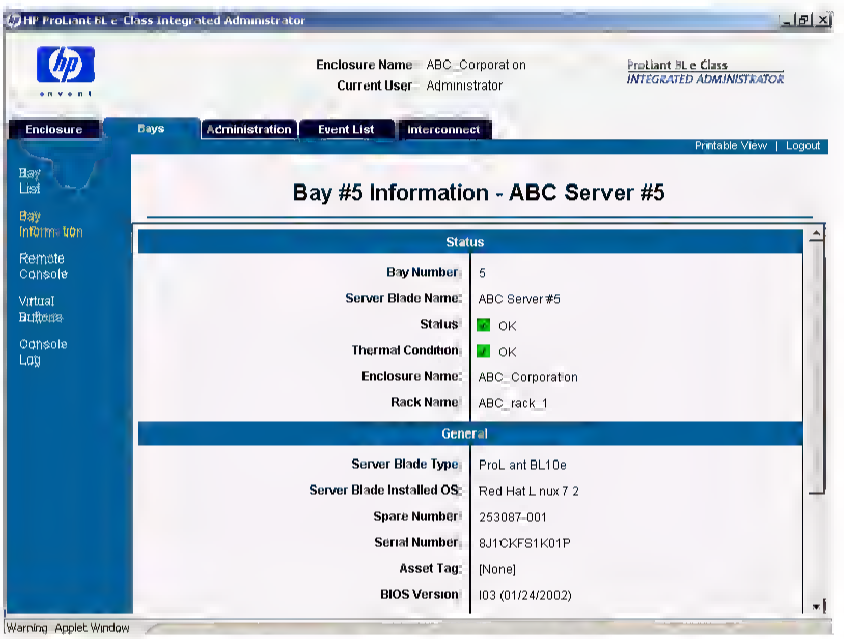


Figure 3-14: Bay Information screen (bay 5 shown)

The **Bay Information** screen enables an enclosure administrator to observe the status and general information for a server blade in a given server blade bay. Group administrators and group members with View rights to the server blade bay can also observe this information.

IMPORTANT: To be sure that the **Bay Information** screen displays the optimal number of possible values, you must have the server blade health driver installed.

Table 3-7 describes the information presented on the **Bay Information** screen for all enclosure administrators and for group members and group with rights to the server blade bay.

Table 3-7: Bay Information Screen

Field	Possible Values	Description
Status Area		
Bay Number		Bay number
Server Blade Name		Name of the server blade as specified with the server blade operating system
Status	OK, Degraded, or Failed	Status of the server blade
Thermal Condition	OK, Warm, Caution, or Critical	Thermal condition of the blade
Enclosure Name		Name of enclosure For the default enclosure name, see Appendix E, "Factory Default Settings."
Rack Name		Name of the rack For the default rack name, see Appendix E, "Factory Default Settings."
General Area		
Server Blade Type		Product name of the server blade
Server Blade Installed OS		Operating system installed on the server blade
Spare Number		Spare number of the server blade
Serial Number		Serial number of the server blade
Asset Tag		Asset tag number of the server blade
BIOS version	mm/dd/yyyy	ROM version on the server blade
CPU # Type		Type of processor on the server blade
CPU # Max. Speed		Speed associated with the server blade processor
Installed RAM		Amount of memory installed on the server blade

continued

Table 3-7: Bay Information Screen *continued*

Field	Possible Values	Description
NIC #1 and #2 MAC Addresses	##:##:##:##:##:##, where ## ranges from 00 to FF.	MAC address of the NIC 1 interface and NIC 2 interface of the server blade

Remote Console

IMPORTANT: If a server blade is running the Microsoft Windows® 2000 operating system, only sequences that occur before the loading of the operating system are visible using Remote Console, unless the server blade is running the HP ProLiant Serial Console for Windows 2000 Server service.

To allow Remote Console access to a server blade, install the HP ProLiant Serial Console for Windows 2000 Server service, located at

www.compaq.com/support/files/server

Enclosure administrators and group administrators with access to the bay can click **Remote Console** to open a remote text-based console to the server blade in the bay.

Figure 3-15 illustrates the information presented on the **Remote Console** screen.

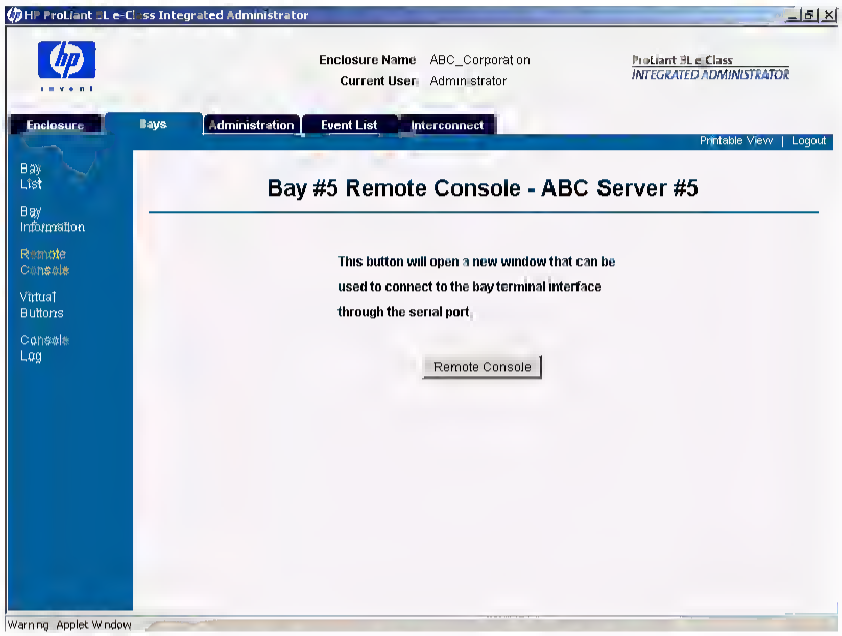


Figure 3-15: Remote Console screen (bay 5 shown)

For information on establishing remote console connectivity, see the "Enabling Remote Console Sessions to Server Blades" section in Chapter 5, "Setting Up the System."

Virtual Buttons

Figure 3-16 illustrates the information in the **Virtual Buttons** screen.

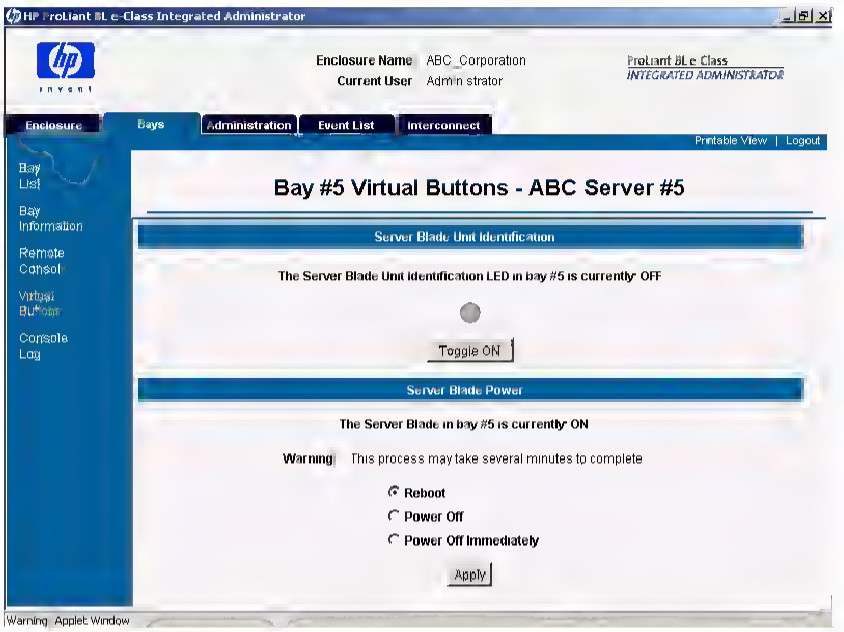


Figure 3-16: Virtual Buttons screen (bay 5 shown)

Enclosure administrators and group administrators with permissions can use tbe **Virtual Buttons** screen to modify the state of the power state and Unit Identification LED of a server blade in order to facilitate troubleshooting from a remote location.

The **Virtual Buttons** screen enables group administrators and enclosure administrators to reboot, power off, or identify the server blade with the following items:

- The **Toggle On/Off** button remotely changes the state of the server blade Unit Identification LED.

- You can select the appropriate function in the Server Blade Power area using the following radio buttons:
  - — **Reboot** reboots the server blade.
  - — **Power Off** attempts a graceful shutdown of the server blade for 5 minutes, after which time this command powers down the server blade immediately.
  - — **Power Off Immediately** powers off the server blade forcefully.

CAUTION: Without the server blade health driver or an ACPI-compliant operating system, the Integrated Administrator cannot gracefully shut down a server blade. This condition can result in the permanent loss of critical data.

IMPORTANT: You must click **Apply** for these settings to take effect.

IMPORTANT: Whenever possible, HP recommends that you use the operating system shutdown procedures before powering down a server blade or enclosure. Once the enclosure is powered off, powering on can only occur with local access to the system.

Console Log

IMPORTANT: Only group members, group administrators, and enclosure administrators can view a console log of a server blade.

The **Console Log** screen displays the console log for the specified bay. The console log of the bay is not stored between reboots of the Integrated Administrator, so the information will only include what has taken place since the last power on of the Integrated Administrator.

The data captured in the console log is all output from the serial console of the server blade that occurred while no one was connected to the console. For security reasons, console output during a user connection session is not logged.

The **Refresh** button refreshes the console log for the current server blade.

Administration Tab

IMPORTANT: For an explanation of user rights associated with the Integrated Administrator, see the "User Permissions" section in Chapter 5, "Setting Up the System."

Under the **Administration** tab, you can access the following screens:

- User List
- Group List
- Add User
- Add Group
- View/Modify User
- View/Modify Group

User List

Figure 3-17 illustrates the information presented in the **User List** screen.

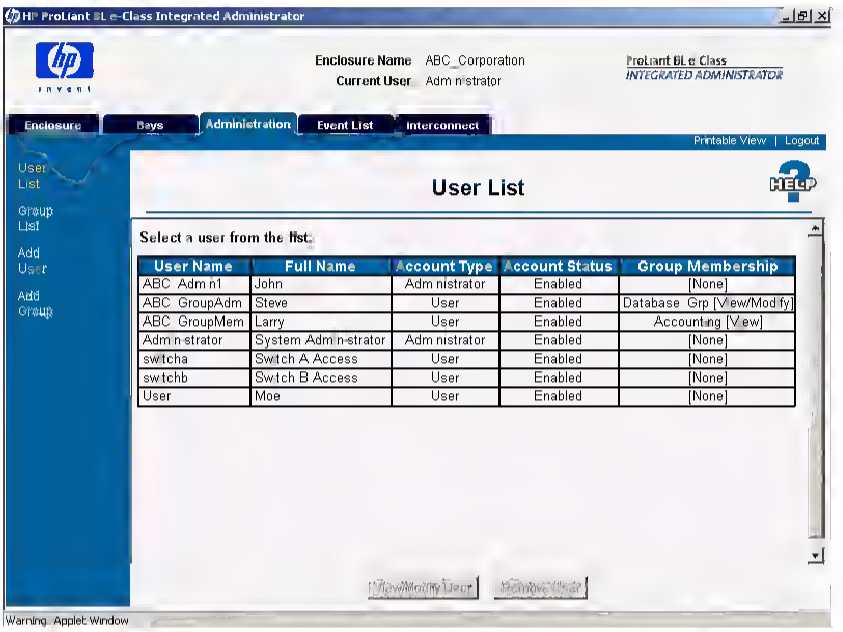


Figure 3-17: User List screen

The **User List** screen enables an appropriate group administrator or enclosure administrator to observe and update user access to groups and server blade bays.

Please note the following permissions related to the action buttons of the **User List** screen (Table 3-8).

Table 3-8: User List Action Buttons and Permissions

Button	Function	Permissions
View/Modify User	Opens the **View/Modify User** screen	Enclosure administrators can access and modify the information for any user. Users can access and modify the information for their own account.
Remove User	Removes the selected user (unless the account is your own)	Only enclosure administrators can execute this command.

Table 3-9 describes the information presented in the **User List** screen.

Table 3-9: User List Screen

Field	Possible Values	Description
User Name		User's login name See Appendix E, "Factory Default Settings," for factory default user accounts.
Full Name		User's full name
Account Type	Administrator or User	Shows if the user is an enclosure administrator
Account Status	Enabled or Disabled	Shows if the user's account is enabled
Group Membership		Shows the groups in which the user has membership

Group List

Figure 3-18 and Table 3-10 describe the information presented in the **Group List** screen.

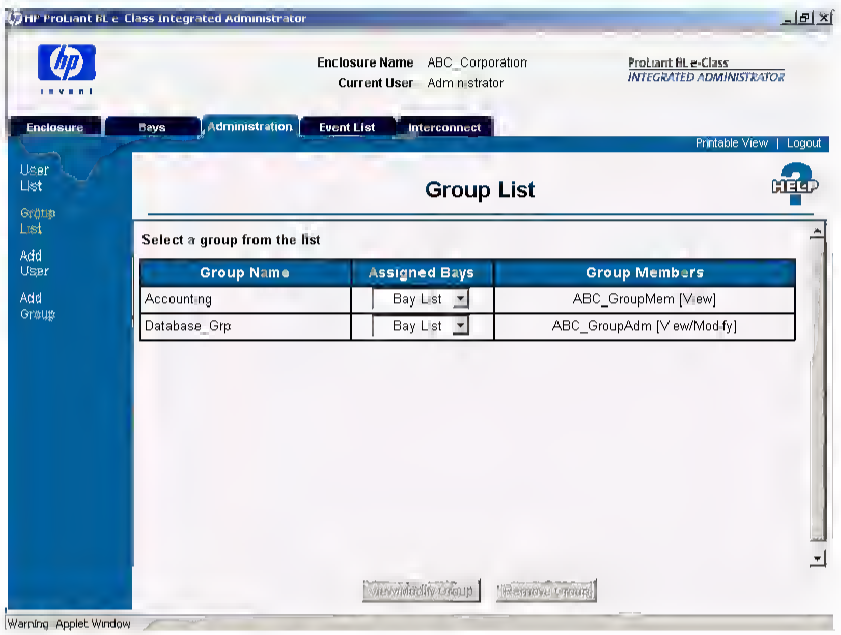


Figure 3-18: Group List screen

The **Group List** screen enables an enclosure administrator to observe and update the assignment of groups and users to server blade bays.

Two buttons appear on this screen:

- **View/Modify Group**—Opens the **View/Modify Group** screen
- **Remove Group**—Removes the selected group

IMPORTANT: Enclosure administrators can view and modify the information for all groups. Group administrators and group members can view the information for the groups in which they are members.

Table 3-10: Group List Screen

Field	Description
Group Name	Group name
Assigned Bays	Server blade bays that the group owns
Group Members	Users with membership in the group

Add User

IMPORTANT: Only enclosure administrators have access to this area of the Integrated Administrator.

Figure 3-19 and Table 3-11 describe the information presented in the User Account area of the **Add User** screen:

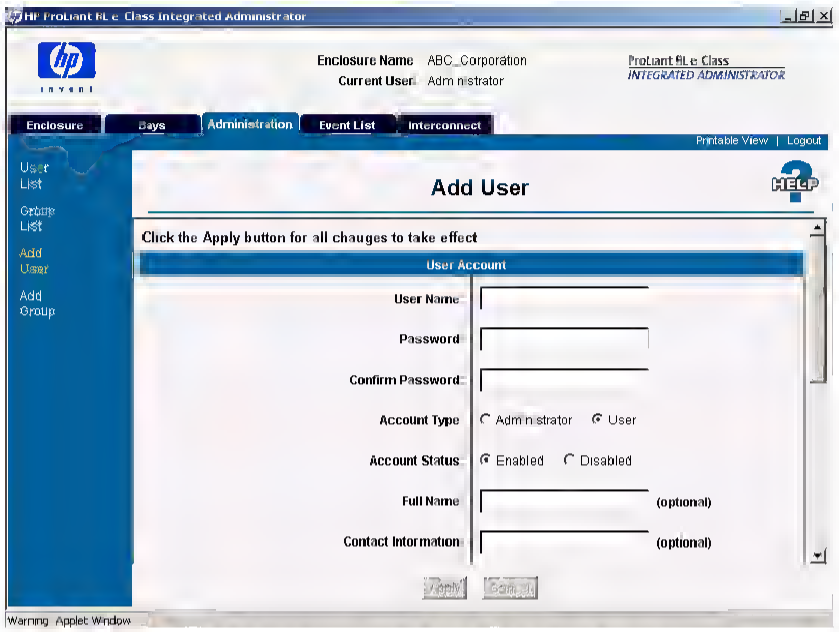


Figure 3-19: Add User screen (User Account area, 1 of 2, shown)

The **Add User** screen enables an enclosure administrator to create a user profile, including group and server blade bays assignments.

Two buttons appear on this screen:

- **Apply**—Saves changes made to this screen
- **Cancel**—Restores all fields on this screen to their original values

Table 3-11: Add User Screen

Field	Possible Values	Description
User Account Area		
User Name	1-13 characters including alphanumeric, dash, and underscore characters The user name must begin with a letter. A maximum of 25 users can be created in addition to the reserved accounts.	Login name of the user. **Note:** "Administrator, "switcha," "switchb," and "all" are reserved names and cannot be used. This restriction is not case-sensitive.
Password	3-8 characters including all printable characters	User's password
Confirm Password	3-8 characters including all printable characters	User's password
Account Type	Radio buttons (Administrator and User)	Determines if the user has enclosure administrator rights
Account Status	Radio buttons (Enabled and Disabled)	Determines if the user's account is enabled
Full Name (optional)	0-20 characters Accepts only alphanumeric, dash, underscore, and space characters	Full name of the user
Contact Information (optional)	0-20 characters Accepts only alphanumeric, dash, underscore, and space characters.	Optional user contact information

continued

Table 3-11: Add User Screen *continued*

Field	Possible Values	Description
Group Membership Area		
Group Names	All groups are listed.	A list of all possible groups
Group Membership	X number of groups (all groups in which the user has membership)	A list of all users that are members of the group
Add User [View] >>>		Adds the user to the selected groups in the Group Names text box with View rights for group members These groups appear in the Group Membership textbox. The user loses View/Modify rights for group administrators if they previously had them.
Add User [View/Modify] >>>		Adds the user to the selected groups in the Group Names text box to the group with View/Modify rights for group administrators or View rights for group members
<<< Remove User		Removes the user from the selected groups in the Group Membership text box

Add Group

IMPORTANT: Only enclosure administrators have access to this area of the Integrated Administrator.

Figure 3-20 illustrates the information presented in the **Add Group** screen.

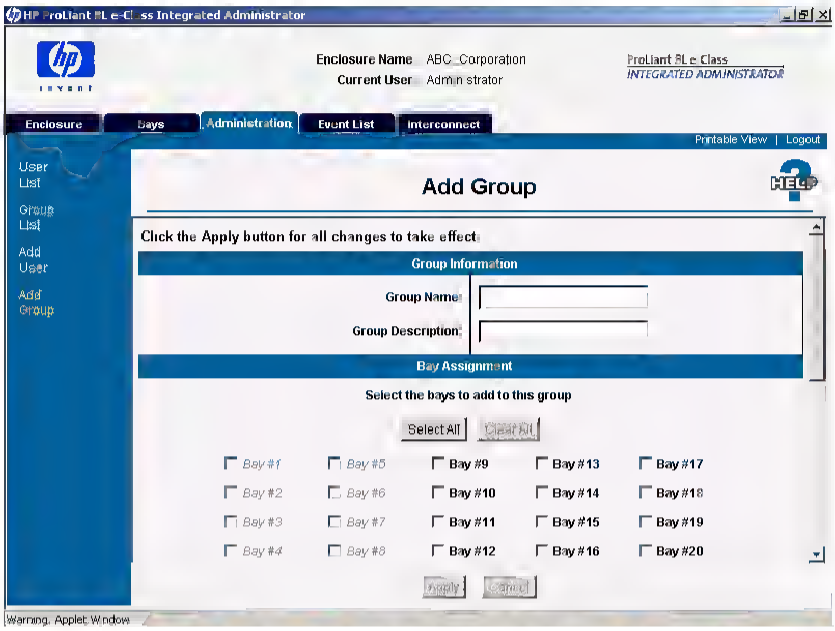


Figure 3-20: Add Group screen (Group Information and Bay Assignment areas, 1 and 2 of 3, shown)

IMPORTANT: Grayed-out checkboxes are unavailable because they are already assigned to another group.

The **Add Group** screen enables an enclosure administrator to create a group profile, including user and server blade bays assignments.

Two buttons appear on this screen:

- **Apply**—Saves changes made to this screen
- **Cancel**—Restores all fields on this screen to their original values

Table 3-12: Add Group Screen

Field	Possible Values	Description
Group Information Area		
Group Name	1-13 characters including alphanumeric, dash, and underscore characters The group name must begin with a letter. A maximum of 20 groups can be created.	Name of group
Group Description (optional)	0-20 characters Accepts only alphanumeric, dash, underscore, and space characters	Description of group
Bay Assignment Area		
Bay 1–Bay 20		Determines which bays the group owns Only one group can own a particular bay. If a checkbox is disabled, another group already owns the bay.
Select All		Selects all checkboxes of the bays
Clear All		Clears all checkboxes of the bays
Group Membership Area		
User Names	All users and enclosure administrators are listed.	A list of all possible users
Group Members	X number of users (all users that are members of the group)	A list of all users that are members of the group

continued

Table 3-12: Add Group Screen *continued*

Field	Possible Values	Description
Group Membership Area, continued		
Add User [View] >>>		Adds selected users in the User Names text box to the group with View rights for group members Users lose View/Modify rights for group administrators if they previously had them.
Add User [View/Modify] >>>		Adds selected users in the User Names text box to the group with View/Modify rights for group administrators
<<< Remove User		Removes selected users in the Group Members text box from the group

View/Modify User

You can access the **View/Modify User** screen by clicking any row in the User List and then clicking **View/Modify User**.

The **View/Modify User** screen provides the same functions and has the same access as the **Add User** screen. See the "Add User" section in this chapter.

View/Modify Group

You can access the **View/Modify Group** screen by clicking any row in the Group List and then clicking **View/Modify Group**.

The **View/Modify Group** screen the provides same functions and has the same access as the **Add Group** screen. See the "Add Group" section in this chapter.

Event List Tab

IMPORTANT: The Event List differs from the System Log in the following ways:

- Any user can view the Event List. Only enclosure administrators can access the System Log.
- The messages in the Event List are limited to cautions and critical failures. Refer to the enclosure System Log for information on both failures and fixes.
- The Event List only displays messages received since the user logged into the Integrated Administrator. The System Log displays every message generated by the enclosure diagnostics.

The Integrated Administrator provides real-time event notifications for an enclosure according to two categories of severity (caution and critical) described in Table 3-13.

Table 3-13: Event Notification Icons

Icon	Description
	Caution—An event that does not prevent the enclosure from operating, maintaining power, or serving its user community When a caution event occurs, a reasonable guarantee that operability can persist no longer exists.
	Critical—An event that prevents the continued operation of the enclosure When a critical event occurs, the inoperability of the enclosure is imminent .

Two buttons appear on this screen:

- **View Event Details**—Navigates to the appropriate screen within the Integrated Administrator to view more details
- **Clear All Events**—Clears all events from event list

Figure 3-21 illustrates the information presented in the **Event List** screen.

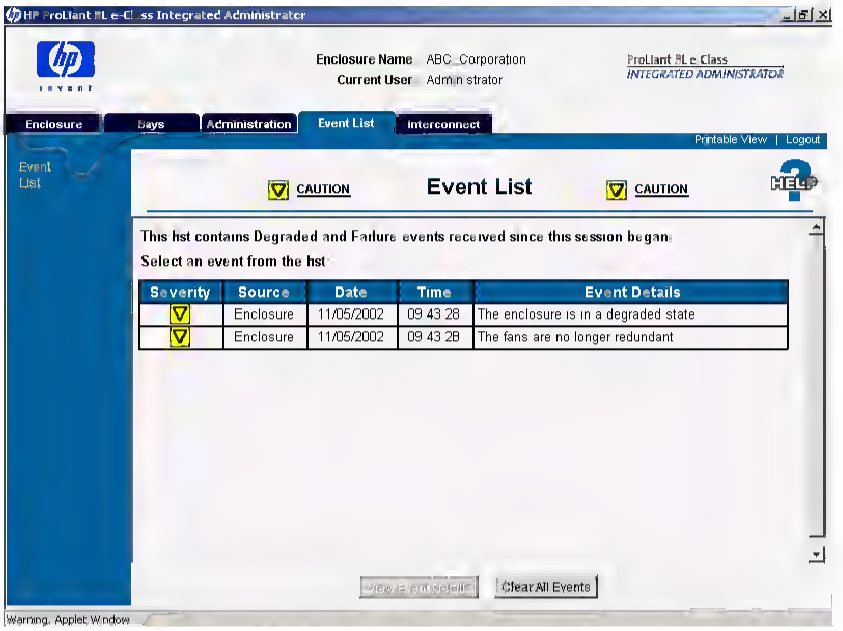


Figure 3-21: Event List screen (fan failure shown)

The **Event List** provides the following information for each event:

- Severity
- Source
- Date
- Time
- Event Details

For detailed information regarding the Event List, including a comprehensive list of event messages, see Appendix D, "Event Details."

Interconnect Tab

Figure 3-22 illustrates the information presented in the **Interconnect Tray** screen:

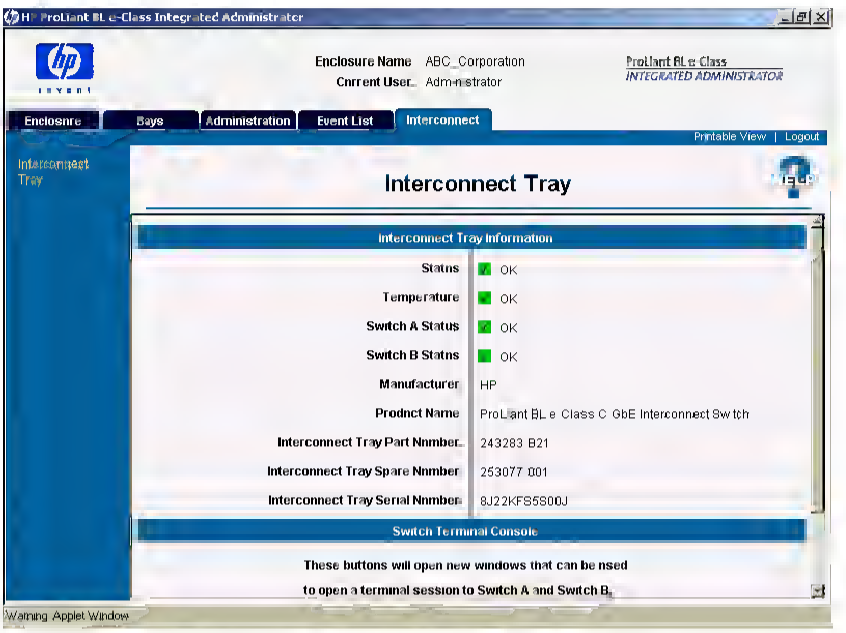


Figure 3-22: Interconnect Tray screen

The **Interconnect Tray** screen allows anyone to view information about the interconnect tray. It allows enclosure administrators to connect to the remote console of one of the interconnect switches if installed.

Table 3-14 describes the information displayed in the areas that comprise the **Interconnect Tray** screen.

Table 3-14: Interconnect Tray screen

Field	Possible Values	Description
Interconnect Tray Information Area		
Status	OK, Degraded, or Failed	Status of the interconnect tray

continued

Table 3-14: Interconnect Tray screen *continued*

Field	Possible Values	Description
Temperature	OK, Warm, Caution, or Critical	Thermal status of the interconnect tray
Switch A Status	OK, Degraded, or Failed	Status of Switch A. This will only be displayed if an interconnect switch is installed.
Switch B Status	OK, Degraded, or Failed	Status of Switch B. This will only be displayed if an interconnect switch is installed.
Manufacturer		Manufacturer of the interconnect tray
Product Name		Product name of the interconnect tray
Interconnect Tray Part Number		Part number for the interconnect tray
Interconnect Tray Spare Number		Spare number for the interconnect tray
Interconnect Tray Serial Number		Serial number for the interconnect tray
Switch Terminal Console Area (only present if an interconnect switch is installed)		
Switch A button		Opens a new window to the remote console of Switch A
Switch B button		Opens a window to the remote console of Switch B

4

Command Line Interface

This chapter provides reference material for operating the Integrated Administrator CLI. This chapter provides command line-related information in the following format:

- Accessing the Command Line Interface
- Operating the command line interface
  - — General commands
  - — General management commands
  - — User account commands
  - — Enclosure network configuration commands
  - — Enclosure management commands
  - — Server bay management commands
- Functionality exclusive to the command line interface

For a detailed explanation of the command line conventions used in this document, see Appendix A, "Command Line Conventions."

For easy reference, tbe index of this book also provides a comprehensive listing of the commands supported by the Integrated Administrator.

Accessing the Command Line Interface

You can access the CLI remotely through the management (10/100 Ethernet) connector or locally through the console (serial) connector on the rear panel of the enclosure.

Accessing Remotely through the Management Connector

To access the Integrated Administrator command line interface remotely through the management (10/100 Ethernet) connector:

1. Get the default host name from the settings tag attached to the interconnect tray.
2. Open a Telnet or Secure Shell application and enter the IP address or DNS name for the enclosure you wish to access.

CAUTION: Using Telnet instead of Secure Shell means your remote session, including password, appears in clear text on that network.

3. Enter the user name and password into the Login prompt.

Accessing Locally through the Console Connector

To access the Integrated Administrator locally through the serial connector:

1. Connect a local client device, such as a laptop computer, to the serial connector using the null-modem cable that ships with the enclosure.

   IMPORTANT: Client devices must satisfy the requirements provided in the "Requirements for Local Client Devices" section in this chapter.

2. Open the terminal emulator and press the **Enter** key to get the login prompt.
3. Enter the user name and password.

Operating the Command Line Interface

General Commands

Table 4-1: General Commands

Command	Description	Restrictions
CLEAR SCREEN	Clears the terminal screen	None
EXIT	Exits the command line interpreter	None
HELP {<command> | TREE}	If a command is given, the usage and help text for the command are shown. If TREE is given, all commands are shown in a tree format. If no argument is given, all base commands are displayed.	None
LOGOUT	Exits the command line interpreter	None
QUIT	Exits the command line interpreter	None
SLEEP <seconds>	Pauses the sessions for a fixed period of time. Useful for adding delays to scripts. The <seconds> field can be any whole number from 1 – 86400. Once the pause has started, no way exists to continue the session before time runs out; but you can terminate the session and start another one.	None

General Management Commands

Table 4-2: General Management Commands

Command	Description	Restrictions
`CLEAR SESSION SWITCH [A | B]`	Terminates a Terminal session from the enclosure. This is not a graceful termination. The connected user loses any unsaved work.	Group administrators may only execute this command for server blade bays to which they have access.
`CLEAR SSHKEY`	Removes the contents of the Secure Shell authorized keys file. After performing this command, you will not be able to login using public key-based authentication.	Only enclosure administrators may execute this command.
`CONNECT SWITCH [A | B]`	Opens a remote console connection to switch A or B. A single switch cannot support multiple simultaneous remote console sessions.	Only enclosure administrators may execute this command.
`DOWNLOAD CERTIFICATE <url>`	Downloads a CA supplied PKCS#7 file to replace the current security certificate on the system. Supported protocols are http, ftp, and tftp. The URL should be formatted as follows: protocol://host/path/file If your ftp server does not support anonymous connections, you can specify a username and password by augmenting the host part in the above format with username:password@host.	Only enclosure administrators may execute this command.
`DOWNLOAD SSHKEY`	Downloands an authorized key file to use with Secure Shell v2 which can contain the public keys for any enclosure administrator. Supported protocols are http, ftp, and tftp. The url should be formatted as protocol://host/path/file. If your ftp server does not support anonymous connections, you can specify a username and password by replacing the host part in the previous format with usemame:password@host.	Only enclosure administrators may execute this command.

continued

Table 4-2: General Management Commands *continued*

Command	Description	Restrictions
GENERATE CERTIFICATE REQUEST	Generates a PKCS#10 certificate request.	Only enclosure administrators may execute this command.
GENERATE CERTIFICATE SELFSIGNED	Generates a self-signed certificate.	Only enclosure administrators may execute this command.
PING {<number>} [<IP address> | <server name>]	Sends ICMP echo messages to a remote IP device. If <number> is omitted, only 5 packets are sent. Packets are sent out at 1-second intervals.	The <IP address> must be in the form ###.###.###.### where ### ranges from 0 to 255.
SET DISPLAY EVENTS [ON | OFF]	Turns event notification on or off The Integrated Administrator preserves this setting across all logins.	None
SET EXPERT {MODE} [ON | OFF]	Turns EXPERT MODE on or off. When EXPERT MODE is turned on, the system will not prompt the user to confirm actions. Users should exercise caution when working in EXPERT MODE as many actions are not reversible.	None
SET FACTORY	Sets the Integrated Administrator back to its factory defaults. The "Administrator" account password does not change. The Integrated Administrator is restarted after all the changes are made. **Note:** This command removes all groups, users, and other customization from the memory of the enclosure, and the information is unrecoverable.	Only the "Administrator" account may execute this account.
SET SCRIPT MODE [ON | OFF]	When SCRIPT MODE is on, all prompting and verifications of entries ceases. If SCRIPT MODE is on, the following commands require a password argument: ADD USER, SET USER PASSWORD, or SET PASSWORD. Default values are used for any parameters that would normally require user interaction.	None

continued

Table 4-2: General Management Commands *continued*

Command	Description	Restrictions
SHOW EXPERT {MODE}:	Displays the current EXPERT MODE setting for the current user.	None
SHOW SESSIONS	Displays the connection to each bay and switch if one exists. Only one user may connect to each bay and switch at a time. It also shows each user that is currently logged in, the user's port number, connect time, and remote system name.	Users may not run this command. Group members and group administrators may only see the sessions for bays assigned to groups to which they belong. Enclosure administrators see all sessions.
SHOW SSHFINGERPRINT	Displays the key fingerprint of the host SSH public key of the Integrated Administrator. This can be used from the serial console to validate the identity of the Integrated Administrator before initializing an SSH connection across a network.	None
SHOW SSHKEY	Displays the contents of the existing Secure Shell authorized keys file that is being used for enclosure administrator key-based authentication.	Only enclosure administrators may execute this command.

User Account Commands

Table 4-3: User Account Commands

Command	Description	Restrictions
ADD GROUP <group name>	Adds a group to the system The default group description is blank.	Only enclosure administrators may execute this command. A maximum of 20 groups may be added to the system. The <group name> must be unique to all other group names and user names and is case-sensitive. It must be 1-13 characters long and can include all alphanumeric, the dash, and the underscore characters. It must begin with a letter. **Note**: Administrator, "switcha," "switchb," and "all" are reserved names and cannot be used. This restriction is not case-sensitive. See Appendix E, "Factory Default Settings," for factory default group accounts.
ADD USER <user name> {<password>}	Adds a user to the system If a password is not given, the user is prompted for one. If SCRIPT MODE is enabled, the password is not optional and must be provided.	Only enclosure administrators may execute this command. A maximum of 25 users may be added in addition to the reserved accounts. The <user name> must be unique to all other user names and group names and is case-sensitive. It must be 1-13 characters long and can include all alphanumeric, the dash, and the underscore characters. The user name must begin with a letter. The <password> must be 3-8 characters long and includes all printable characters. If a password is not entered, the user is prompted for one. **Note**: Administrator, "switcha," "switchb," and "all" are reserved names and cannot be used. This restriction is not case-sensitive. See Appendix E, "Factory Default Settings," for factory default user accounts.

continued

Table 4-3: User Account Commands *continued*

Command	Description	Restrictions
`ASSIGN ADMINISTRATOR {RIGHTS} <user name>`	Promotes a user to have enclosure administrator permissions Group membership is not deleted in case enclosure administrator rights are removed at a later time.	Only enclosure administrators may execute this command. The <user name> is case-sensitive.
`ASSIGN BAY [ALL | <bay number> {[ , | -] <bay number>}] <group name>`	Assigns one or more bays to a group If a bay is already assigned to a group, it must first be unassigned before executing this command.	Only enclosure administrators may execute this command. The <group name> is case-sensitive.
`ASSIGN USER <user name> <group name> {[VIEW | MODIFY]}`	Assigns a user to a group with View rights (for group members) or View/Modify rights (for group administrators) If View or View/Modify is not specified, View is chosen by default.	Only enclosure administrators may execute this command. The <user name> and <group name> are case-sensitive. The "Administrator" account cannot be added to a group.
`DISABLE USER <user name>`	Disables a user account The user is immediately logged out of the system and prevented from log in until the account is enabled.	Only enclosure administrators may execute this command. The <user name> is case-sensitive. The "Administrator" account cannot be disabled.
`ENABLE USER <user name>`	Enables a user account that was previously disabled by the DISABLE USER command	Only enclosure administrators may execute this command. The <user name> is case-sensitive.
`REMOVE GROUP [ALL | <group name>]`	Removes a group and automatically unassigns all bays within the group	Only enclosure administrators may execute this command. The <group name> is case-sensitive.

continued

Table 4-3: User Account Commands *continued*

Command	Description	Restrictions
`REMOVE USER [ALL | <user name>]`	Removes a user from the system If ALL is specified, the command is run for all users except the default system accounts.	Only enclosure administrators may execute this command. The <user name> is case-sensitive. The "Administrator," "switcha," and "switchb" accounts cannot be removed.
`SET GROUP {DESCRIPTION} <group name> <description>`	Sets a group's description.	Only enclosure administrators may execute this command. The <group name> is case-sensitive. The <description> must be 0-20 characters long and can include all alphanumeric characters, the dash, the underscore, and spaces. The default group description is blank. If spaces are part of the contact information, enclose the information in quotes.
`SET PASSWORD {<password>}`	Sets the password of the user currently logged into the Integrated Administrator. If a password is not given on the command line, the user is prompted for one. **Note:** This command is not valid in SCRIPT MODE if password is not specified.	The <password> must be 3-8 characters long and can include all printable characters.

continued

Table 4-3: User Account Commands *continued*

Command	Description	Restrictions
`SET USER CONTACT {<user name>} <contact info>`	If no <user name> exists, the command modifies the contact info of the user that executed the command.	Only enclosure administrators may modify another user's contact information. The <user name> is case-sensitive. The <contact info> must be 0-20 characters long and can include all alphanumeric characters, the dash, the underscore, and spaces. The default contact information is blank. If spaces are part of the contact information, enclose the information in quotes.
`SET USER FULLNAME {<user name>} <full name>`	Sets a user's full name. If no <user name> exists, the command modifies the full name of the user that is currently logged in.	Only enclosure administrators may modify another user's full name. The <user name> is case-sensitive. The <full name> must be 0-20 characters long and can include all alphanumeric, the dash, the underscore, and space characters. The default full name is blank. If spaces are part of this information, enclose the information in quotes.
`SET USER PASSWORD <user name> {<new password>}`	Sets a user's password. If you do not supply a password on the command line, you are prompted for one. **Note:** This command is not valid in SCRIPT MODE if password is not specified.	Only enclosure administrators may modify another user's password. Only the "Administrator" account may modify the password of the "Administrator" account. The <user name> is case-sensitive. The <new password> must be 3-8 characters long and can include all printable characters.

continued

Table 4-3: User Account Commands *continued*

Command	Description	Restrictions
SHOW GROUP [<group name> | ALL]	Displays the group's description, a list of members with View permission, a list of members with View/Modify permission, number of bays, and a list of each of the bays the group manages. If ALL is entered, the command is run for every group, and displays the group description and the number of assigned users and bays.	Group members and group administrators only see the groups in which they have membership. Users may not execute this command. The <group name> is case-sensitive. If spaces are part of this information, enclose the information in quotes.
SHOW USER [<user name> | ALL]	Displays the user's full name, contact, whether the user has administrator rights, whether the account is enabled, and the groups for which the user has View or View/Modify permissions. If ALL is entered, this information is given for every user and an asterisk before the user name denotes the current user.	Only enclosure administrators may view another user's information. The <user name> is case-sensitive. Users who do not have enclosure administrator permissions only see their user information.
UNASSIGN ADMINISTRATOR {RIGHTS} <user name>	Takes enclosure administrator rights from a user.	Only enclosure administrators may execute this command. The "Administrator" account cannot have enclosure administrator rights taken away. The <user name> is case-sensitive.
UNASSIGN USER <user name> <group name>	Removes the user from the specified group.	Only enclosure administrators may execute this command. The <user name> and <group name> are case-sensitive.

Enclosure Network Configuration Commands

Table 4-4: Enclosure Network Configuration Commands

Command	Description	Restrictions
ADD SNMP TRAPRECEIVER <IP address>	Adds an IP address to receive SNMP traps. Only v1 traps are supported. Traps are directed to the SNMP default port, 162.	Only enclosure administrators may execute this command. A maximum of 8 IP address may be added to receive SNMP traps. The <IP address> must be in the form ###.###.###.### where ### ranges from 0 to 255.
DISABLE SECURESH	Disables Secure Shell access to the Integrated Administrator. Disabling Secure Shell prevents access to the Web-based user interface and the Secure Shell terminal interface until a terminal session re-enables the Secure Shell protocol.	Only enclosure administrators may execute this command.
DISABLE SNMP	Disables SNMP support for the Integrated Administrator. Does not clear the SNMP trap receivers that have been configured. SNMP trap receivers can still be added and removed. If SNMP is disabled, Insight Manager agents do not work properly.	Only enclosure administrators may execute this command.
DISABLE TELNET	Disables Telnet access to the Integrated Administrator.	Only enclosure administrators may execute this command.
DISABLE WEB	Disables HTTP and HTTPS access to the Integrated Administrator. This command prevents access to the Web-based user interface.	Only enclosure administrators may execute this command.

continued

Table 4-4: Enclosure Network Configuration Commands *continued*

Command	Description	Restrictions
DOWNLOAD CONFIG <url>	Downloads a previously saved configuration file from a specific IP host The files are auto-executed in script mode. The file is not allowed to change the password of the "Administrator" account. Supported protocols are http, ftp, and tftp. The URL should be formatted as protocol://host/path/file. If your ftp server does not support anonymous connections, you can specify a username and password by replacing the host part in the previous format with username:password@host.	Only enclosure administrators may execute this command. The IP address must be in the form ###.###.###.### where ### ranges from 0 to 255.
ENABLE SECURESH	Enables Secure Shell support for the Integrated Administrator	Only enclosure administrators may execute this command.
ENABLE SNMP	Enables SNMP support for the Integrated Administrator	Only enclosure administrators may execute this command.
ENABLE TELNET	Enables Telnet access to the Integrated Administrator	Only enclosure administrators may execute this command.
ENABLE WEB	Enables HTTP and HTTPS access to the Integrated Administrator	Only enclosure administrators may execute this command.
REMOVE SNMP TRAPRECEIVER <IP address>	Removes an IP address from the list of systems to receive SNMP traps	Only enclosure administrators may execute this command. The IP address must be in the form ###.###.###.### where ### ranges from 0 to 255.
SET DNS <primary address> {<secondary address>}	Sets the primary and secondary DNS server addresses These servers are only used if the system is currently configured to use a static IP address.	Only enclosure administrators may execute this command. The <primary address> and <secondary address> must be in the form ###.###.###.### where ### ranges from 0 to 255.

continued

Table 4-4: Enclosure Network Configuration Commands *continued*

Command	Description	Restrictions
`SET GATEWAY <IP address>`	Sets the network default gateway This gateway is only used if the system is configured to use a static IP address.	Only enclosure administrators may execute this command. The <IP address> needs to be in the form ###.###.###.### where each ### ranges from 0 to 255.
`SET IPCONFIG [DHCP {DYNAMICDNS} | STATIC <IP address> <netmask>]`	Sets up the Integrated Administrator IP configuration The gateway and DNS addresses are cleared. The optional DYNAMICDNS argument enables Dynamic DNS.	Only enclosure administrators may execute this command. The <IP address> and <netmask> need to be in the form ###.###.###.### where each ### ranges from 0 to 255.
`SET SNMP COMMUNITY [READ | WRITE] <community name>`	Sets the community name for the read or write SNMP community The default names for the read and write community are "public" and blank, respectively. If a blank write community name is given, SNMP set commands are disabled until a non-empty community name is given.	Only enclosure administrators may execute this command. The write <community name> must be 0-20 characters long, and the read <community name> must be 1-20 characters long. Both include all alphanumeric, the underscore, and the dash characters. The default read community name is "public." The default write community name is blank.
`SET SNMP CONTACT <contact>`	Configures the name of the system contact The default contact is blank.	Only enclosure administrators may execute this command. The <contact> must be 0-20 characters long and includes all alphanumeric characters, the underscore, the dash, and the space. If spaces are part of this information, enclose the information in quotes.

continued

Table 4-4: Enclosure Network Configuration Commands *continued*

Command	Description	Restrictions
`SET SNMP LOCATION <location>`	Configures the SNMP location of the enclosure. The default location is blank.	Only enclosure administrators may execute this command. The <location> must be 0-20 characters long and includes all alphanumeric characters, the underscore, the dash, and the space. If spaces are part of this information, enclose the information in quotes.
`SHOW NETWORK`	Displays the DHCP state, Dynamic DNS state, IP address, subnet mask, gateway address, primary and secondary DNS addresses, MAC address, HTTP and HTTPS server status, SNMP status, Secure Shell status, and Telnet status of the enclosure.	None
`SHOW SNMP`	Displays the SNMP system name, location, and contact; read community name; write community name; and a list of the trap destinations.	Only enclosure administrators may execute this command.

Enclosure Management Commands

Table 4-5: Enclosure Management Commands

Command	Description	Restrictions
`CLEAR SYSLOG ENCLOSURE`	Clears the enclosure system log	Only enclosure administrators may execute this command. Once deleted, this information cannot be restored.
`POWEROFF ENCLOSURE {FORCE}`	Performs a graceful shutdown of the enclosure. Each blade is first gracefully shutdown. If the FORCE argument is given, the enclosure and all blades are immediately shutdown.	Only enclosure administrators may execute this command.
`RESTART`	Restarts the Integrated Administrator. This does not affect current operation of bays in the system.	Only enclosure administrators may execute this command.
`SET DATE MMDDhhmm {{CC}YY} {TZ}`	Sets the date of the enclosure with the following definitions: • *MM*: month • *DD*: day • *hh*: hour (24-hour time) • mm: minute • *CC*: century • *YY*: year • *TZ*: time zone (case-sensitive) If the time zone is left blank, the current time zone is left in effect.	Only enclosure administrators may execute this command. • *MM* is an integer from 1-12. • *DD* is an integer from 1-31. • *hh* is an integer from 0-23. • mm is an integer from 0-59. For a list of time zones, see Appendix F, "Time Zone Settings." NTP must be disabled before manually setting the date and time.

continued

Table 4-5: Enclosure Management Commands *continued*

Command	Description	Restrictions
`SET ENCLOSURE ASSET {TAG} <asset tag>`	Changes the enclosure asset tag	Only enclosure administrators may execute this command. The <asset tag> must be 1-31 characters long and includes alphanumeric, dash, and underscore characters. The default enclosure asset tag is blank. To set a blank asset tag, specify the blank value using quotes.
`SET ENCLOSURE NAME <enclosure name>`	Changes the enclosure name	Only enclosure administrators may execute this command. The <enclosure name> must be 1-32 characters long and includes all alphanumeric, the dash, and the underscore characters. The default enclosure name is IA-MAC where MAC is replaced with the actual MAC address.
`SET ENCLOSURE UID [ON | OFF]`	Turns the enclosure Unit Identification LED on or off	Only enclosure administrators may execute this command.
`SET RACK NAME <rack name>`	Sets the name for the rack where the enclosure resides	Only enclosure administrators may execute this command. The <rack name> must be 1-32 characters long and includes all alphanumeric, dash, and underscore characters. The default rack name is "UnnamedRack."
`SHOW CONFIG`	Displays the script required to recreate the settings of the enclosure Passwords are not included for any user.	Only enclosure administrators may execute this command.

continued

Table 4-5: Enclosure Management Commands *continued*

Command	Description	Restrictions
SHOW DATE	Displays the current date, time, and time zone of the internal clock of the enclosure.	None
SHOW DISPLAY EVENT	Displays whether event notification is on or off.	None
SHOW ENCLOSURE FAN [<fan number> | ALL]	Displays the status, redundancy, partner, speed, and part number for the requested fan. If ALL is entered, this information is shown for all fans.	None
SHOW ENCLOSURE INFO	Displays the enclosure name, type, part number, serial number, and asset tag; the Integrated Administrator software and hardware version; Integrated Administrator MAC address; and the interconnect tray type, part number, and serial number.	None
SHOW ENCLOSURE POWERSUPPLY [<power supply number> | ALL]	Displays the power supply status, AC input status, capacity, input voltage range #1 (measured in Volts), input voltage range #2 (if necessary, measured in Volts), input frequency range (measured in Hertz), part number, serial number, and hardware revision for the specified power supply if one is specified or for all power supplies if ALL is given.	None
SHOW ENCLOSURE STATUS	Under an enclosure status heading, this command displays the health, Integrated Administrator health, and unit identification LED of the enclosure. Under a power status heading, this command displays the power status and capacity.	None

continued

Table 4-5: Enclosure Management Commands *continued*

Command	Description	Restrictions
`SHOW ENCLOSURE TEMP`	Displays the locale, status (OK, warm, degraded, or failed), temperature in degrees Fahrenheit, and temperature in degrees Celsius for all temperature sensors.	None
`SHOW RACK NAME <rack name>`	Shows the name for the rack where the enclosure resides. The default rack name is "UnnamedRack."	None
`SHOW SYSLOG ENCLOSURE`	Displays the syslog of the enclosure with 22 lines per screen. Typing "q" quits the command; any other key shows the next screen if more information exists to display. Typing "c" continuously displays the System Log without page breaks.	Only enclosure administrators may execute this command.
`SHOW TRAY INFO`	Displays the manufacturer, product name, part number, serial number, and spare number of the interconnect tray.	None
`UPDATE IMAGE <url>`	Downloads a new image from a server over the network and uses the image to upgrade the firmware of the enclosure.	Only enclosure administrators may execute this command. <URL> can be any of the following: • http://*host*/path • tftp://*host*/path • ftp://username:password @*host*/path • ftp://*host*/path where host is a fully qualified domain name or an IP address and path is the pathname of the flash image to download.

continued

Table 4-5: Enclosure Management Commands *continued*

Command	Description	Restrictions
`UPLOAD CONFIG <url>`	Uploads the current runtime configuration to the specified FTP or TFTP server.	Only enclosure administrators may execute this command.

Server Bay Management Commands

Table 4-6: Server Bay Management Commands

Command	Description	Restrictions
`CLEAR BAY BOOT [FIRST | ONCE] [ALL | <bay number> {[ , - ] <bay number>}]`	Clears the setting for the IPL to be passed to the blade at the next reboot. The "FIRST" argument resets the IPL for all subsequent reboots. The "ONCE" argument resets the IPL for the next reboot only. This command is only valid for present blades. This command requires BIOS version 06/15/02 or greater for the ProLiant BL10e server blade ROM.	Only enclosure and group administrators may execute this command.
`CLEAR SESSION BAY <bay number>`	Terminates a Terminal session from the enclosure. This is not a graceful termination. The connected user loses any unsaved work.	Enclosure administrators may execute this command for server blade bays and the interconnect switch.
`CONNECT BAY <bay number>`	Opens a remote console session to the server blade with that server blade bay number. A server blade can only support one remote console session at a time.	Only enclosure and group administrators may execute this command.

continued

Table 4-6: Server Bay Management Commands *continued*

Command	Description	Restrictions
`GENERATE NMI <bay number>`	Generates an NMI on the specified blade. The consequences of an NMI are operating system specific.	Only enclosure and group administrators may execute this command.
`POWEROFF BAY <bay number> {[ , | - ] <bay number>} {FORCE}`	Performs a graceful shutdown of the server blade in the specified bay. If the FORCE argument is given, the server blade is immediately shut down. This means the server blade could lose data or become unstable. If no server blade is in the specified bay, the user is told that the bay is empty.	Only enclosure and group administrators may execute this command.
`POWERON BAY <bay number> {[ , | - ] <bay number>} {[PXE | HDD | RBSU]}`	Powers on the specified server blade. If no server blade is in the specified bay, the user is told that the bay is empty. The optional boot arguments require a BIOS version of 06/15/02 or greater of the ProLiant BL10e Server blade ROM. Adding an optional boot argument forces the blade to abandon the regular boot order and forces a boot using the specified method.	Only enclosure and group administrators may execute this command.

continued

Table 4-6: Server Bay Management Commands *continued*

Command	Description	Restrictions
`REBOOT BAY <bay number> {[ , | - ] <bay number>} {FORCE} {[PXE | HDD | RBSU]}`	Sends a request to the server blade to perform a graceful shutdown. The server blade is then powered on. If no server blade is in the specified bay, the user is told that the bay is empty. The optional boot arguments require a BIOS version of 06/15/02 or greater of the ProLiant BL10e Server blade ROM. Adding an optional boot argument forces the blade to abandon the regular boot order and forces a boot using the specified method.	Only enclosure and group administrators may execute this command.
`SET BAY BOOT FIRST [HDD | PXE] <bay number> {[ , | - ] <bay number>}`	Sets the IPL for each subsequent reboot. This setting is only valid for present blades and is cleared if a blade is removed. This command requires BIOS version 06/15/02 or greater for the ProLiant BL10e server blade ROM.	Only enclosures and administrators may execute this command.
`SET BAY BOOT ONCE [HDD | PXE | RBSU] <bay number> {[ , | - ] <bay number>}`	Sets the boot device to be used on the next boot of the bay(s) specified. This setting is only valid on present blades and is cleared if the blade is removed. This command requires BIOS version 06/15/02 or greater for the ProLiant BL10e server blade ROM.	Only enclosure and administrators may execute this command.

continued

Table 4-6: Server Bay Management Commands *continued*

Command	Description	Restrictions
`SET BAY UID <bay number> {[ , | - ] <bay number>} [ON | OFF]`	Turns a Unit Identification LED on the server blade on or off.	Only enclosure and group administrators may execute this command.
`SHOW BAY INFO [ALL | <bay number> {[ , | - ] <bay number>}]`	Displays the following fields: Assigned to group, type, name, installed operating system, part number, serial number, asset tag, BIOS version, all CPU types and associated maximum speeds, memory, NIC #1 MAC, and NIC #2 MAC. If no server is in the bay, the user is shown the assigned to group and the server blade type.	Group members and group administrators only see information for the bays in their groups.
`SHOW BAY LIST [ALL | <group name>]`	Displays the assigned to group, remote console user, and server blade name for each bay in a particular group if a group name is specified or all bays if ALL is specified	Group members and group administrators only see information for the bays in their groups.
`SHOW BAY STATUS [ALL | <bay number> {[ , | - ] <bay number>}]`	Displays the power (On or Off), assigned to group, remote console user, health (OK, CPU failure, or power module failure), thermal (OK, warm, degraded, or failed), and Unit Identification LED (On or Off) for the server blade.	Group members and group administrators only see information for the bays in their groups.

continued

Table 4-6: Server Bay Management Commands *continued*

Command	Description	Restrictions
`SHOW SYSLOG BAY <bay number>`	Displays the syslog of the specified blade with 22 lines per screen. Typing "q" quits the command; any other key shows the next screen if more information is available to display. The system log of the server blade is not stored between reboots, so the information only includes what has taken place since the last power on of the Integrated Administrator. Typing "c" continuously displays the System Log without page breaks.	Group members and group administrators only see information for the bays in their groups.
`UNASSIGN BAY [ALL | <bay number> {[ , | - ] <bay number>}]`	Removes the bay(s) from their assigned group.	Only enclosure administrators may execute this command.

Command Line Event Messages

Table 4-7: Command Line Event Messages

Message	Possible Cause
User Event Messages	
User Permission Change	One of the following has occurred: • A user has been added, removed, or modified. • A user's group membership has been modified. The server blade bay membership has been changed for a group with at least one user.
Enclosure Event Messages	
Enclosure Shutdown	The enclosure is being shutdown.
Enclosure Status Change	The Integrated Administrator detected a change in status due to a change in the state of one or more hardware components or server blade readings.
Fan Inserted	A fan has been inserted.
Fan Removed	A fan has been removed.
Fan Status Change	The status of a fan has changed.
Power Supply Inserted	A power supply has been inserted.
Power Supply Overload	The power subsystem is overloaded. Check each power supply status to determine cause.
Power Supply Redundancy Change	The power supplies are now either redundant or no longer redundant.
Power Supply Removed	A power supply has been removed.
Power Supply Status Change	The status of a power supply has changed.
Restart Event	The Integrated Administrator is about to restart.
Thermal Status Change	The state of a thermal sensor has changed.

continued

Table 4-7: Command Line Event Messages *continued*

Message	Possible Cause
Bay Event Messages	
Bay Event	A server blade bay has been assigned or unassigned from a group.
Blade Inserted	A server blade was inserted into the enclosure.
Blade Removed	A server blade was removed from the enclosure.
Blade Status Change	Health driver detected a change in status due to a change in the state of one or more hardware components or server blade readings.

Functionality Exclusive to the Command Line Interface

Table 4-8 identifies functions or capabilities available to the command line interface and unavailable when using the Web-based user interface.

Table 4-8: Functionality Exclusive to the Command Line Interface

Function	Description	Capability Exclusive to the Command Line Interface
General Commands		
`SLEEP <seconds>`	Pauses the sessions for a fixed period of time. Useful for adding delays to scripts. The <seconds> field can be any whole number from 1 – 86400. Once the pause has started, no way exists to continue the session before time runs out, but you can terminate the session and start another one.	None
General Management Commands		
`CLEAR SESSION SWITCH [A | B]`	Terminates a Terminal session from the enclosure This is not a graceful termination. The connected user loses any unsaved work.	All
`CLEAR SSHKEY`	Removes the contents of the Secure Shell authorized keys file. After performing this command, you will not be able to login using public key-based authentication.	Only enclosure administrators may execute this command.

continued

Table 4-8: Functionality Exclusive to the Command Line Interface *continued*

Function	Description	Capability Exclusive to the Command Line Interface
General Management Commands, continued		
DOWNLOAD CERTIFICATE <url>	Downloads a CA supplied PKCS#7 file to replace the current security certificate on the system. Supported protocols are http, ftp, and tftp. The URL should be formatted as protocol://host/path/file. If your ftp server does not support anonymous connections, you can specify a username and password by augmenting the host part in the above format with username:password@host.	All
DOWNLOAD SSHKEY	Downloads an authorized key file to use with Secure Shell v2 which can contain the public keys for any enclosure administrator. Supported protocols are http, ftp, and tftp. The url should be formatted as protocol://host/path/file. If your ftp server does not support anonymous connections, you can specify a username and password by replacing the host part in the previous format with username:password@host.	Only enclosure administrators may execute this command.
GENERATE CERTIFICATE REQUEST	Generates a PKCS#10 certificate request	All
GENERATE CERTIFICATE SELFSIGNED	Generates a self-signed certificate	All

continued

Table 4-8: Functionality Exclusive to the Command Line Interface *continued*

Function	Description	Capability Exclusive to the Command Line Interface
General Management Commands, continued		
`PING {<number>} [<IP address> | <server name>]`	Sends ICMP echo messages to a remote IP device If <number> is omitted, only 5 packets are sent. Packets are sent out at 1-second intervals.	All
`SET DISPLAY EVENTS [ON | OFF]`	Turns event notification on or off The Integrated Administrator preserves this setting across all log-ins.	All
`SET EXPERT {MODE} [ON | OFF]`	Turns EXPERT MODE on or off. When EXPERT MODE is turned on, the system will not prompt the user to confirm actions. Users should exercise caution when working in EXPERT MODE as many actions are not reversible.	None
`SET FACTORY`	Sets the Integrated Administrator back to its factory defaults The password of the "Administrator" account does not change. The Integrated Administrator is restarted after all the changes are made. **Note:** This command removes all groups, users, and other customization from the memory of the enclosure, and the information is unrecoverable.	All

continued

Table 4-8: Functionality Exclusive to the Command Line Interface *continued*

Function	Description	Capability Exclusive to the Command Line Interface
General Management Commands, continued		
SET SCRIPT MODE [ON | OFF]	When SCRIPT MODE is on, all prompting and verifications of entries cease. If SCRIPT MODE is on, the following commands require a password argument: ADD USER, SET USER PASSWORD, or SET PASSWORD. An enclosure administrator must change the password so that the user can log in to the system. Default values are used for any parameters that would normally require user interaction.	All
SHOW EXPERT {MODE}:	Displays the current EXPERT MODE setting for the current user.	None
SHOW SESSIONS	Displays the connection to each bay and switch if one exists. Only one user may connect to each bay and switch at a time. It also shows the users that are currently logged in, their port number, connect time, and remote system name.	All
SHOW SSHFINGERPRINT	Displays the key fingerprint of the host SSH public key for the Integrated Administrator. This can be used from the serial console to validate the identity of the Integrated Administrator before initializing an SSH connection across a network.	None
SHOW SSHKEY	Displays the contents of the existing Secure Shell authorized keys file that is being used for enclosure administrator key-based authentication.	Only enclosure administrators may execute this command.

continued

Table 4-8: Functionality Exclusive to the Command Line Interface *continued*

Function	Description	Capability Exclusive to the Command Line Interface
General Management Commands, continued		
`DOWNLOAD CONFIG <url>`	Downloads a previously saved configuration file from a specific IP host. The file is auto-executed in SCRIPT MODE. The file is not allowed to change the password of the "Administrator" account. Supported protocols are http, ftp, and tftp. The URL should be formatted as protocol://host/path/file. If your ftp server does not support anonymous connections, you can specify a username and password by replacing the host part in the previous format with username:password@host.	All
Enclosure Management Commands		
`SHOW CONFIG`	Displays the script required to recreate the settings of the enclosure. Passwords are not included for any user.	All
`SHOW ENCLOSURE FAN [<fan number> | ALL]`	Displays the status, redundancy, partner, speed, and part number for the requested fan. If ALL is entered, this information is shown for all fans.	The command line adds the fan partner.

continued

Table 4-8: Functionality Exclusive to the Command Line Interface *continued*

Function	Description	Capability Exclusive to the Command Line Interface
Enclosure Management Commands, continued		
SHOW ENCLOSURE POWERSUPPLY [<power supply number> | ALL]	Displays the status of the power supply, AC input status, capacity, input voltage range #1 (measured in Volts), input voltage range #2 (measured in Volts), input frequency range (measured in Hertz), part number, serial number, and hardware revision for the specified power supply if one is specified or for all power supplies if ALL is given.	The command line adds the input voltage ranges, input frequency range, serial number, and hardware revision.
SHOW ENCLOSURE STATUS	Under an enclosure status heading, this command displays the health of the enclosure, Integrated Administrator health, and unit identification LED. Under a power status heading, this command displays the power status and capacity.	The command line adds the Integrated Administrator health
UPDATE IMAGE <URL>	Downloads a new image from a server over the network and uses the image to upgrade the firmware of the enclosure.	All
UPLOAD CONFIG <url>	Uploads the current runtime configuration to the specified FTP or TFTP server.	All
CLEAR SESSION BAY <bay number>	Terminates a Terminal session from the enclosure. This is not a graceful termination. The connected user loses any unsaved work.	All

continued

Table 4-8: Functionality Exclusive to the Command Line Interface *continued*

Function	Description	Capability Exclusive to the Command Line Interface
Enclosure Management Commands, continued		
`CLEAR BAY BOOT [FIRST | ONCE] [ALL | <bay number> {[ , | - ] <bay number>}]`	Clears the setting for the IPL to be passed to the blade at the next reboot. The "FIRST" argument resets the IPL for all subsequent reboots. The "ONCE" argument resets the IPL for the next reboot only. This command is only valid for present blades. This command requires BIOS version 06/15/02 or greater for the ProLiant BL10e server blade ROM.	Only enclosure and group administrators may execute this command.
`GENERATE NMI <bay number>`	Generates an NMI on the specified blade. The consequences of an NMI are operating system specific.	All
`POWERON BAY <bay number> {[ , | - ] <bay number>} {[PXE | HDD | RBSU]}`	Powers on the specified server blade. If no server blade is in the specified bay, the user is told that the bay is empty. The optional book arguments require a BIOS version of 06/15/02 or greater of the ProLiant BL10e Server blade ROM. Adding an optional boot argument forces the blade to abandon the regular boot order and forces a boot using the specified method.	Allows for optional boot argument

continued

Table 4-8: Functionality Exclusive to the Command Line Interface *continued*

Function	Description	Capability Exclusive to the Command Line Interface
Enclosure Management Commands, continued		
`REBOOT BAY <bay number> {[ , | - ] <bay number>} {FORCE} {[PXE | HDD | RBSU]}`	Sends a request to the server blade to perform a graceful shutdown. The server blade is then powered on. If no server blade is in the specified bay, the user is told that the bay is empty. The optional boot arguments require a BIOS version of 06/15/02 or greater of the ProLiant BL10e Server blade ROM. Adding an optional boot argument with force the blade to abandon the regular boot order and force a boot using the specified method.	Allows for optional boot argument
`SET BAY BOOT FIRST [HDD | PXE] <bay number> {[ , | - ] <bay number>}`	Sets the IPL for each subsequent reboot. This setting is only valid for present blades and is cleared if a blade is removed. This command requires BIOS version 06/15/02 or greater for the ProLiant BL10e server blade ROM.	Only enclosures and administrators may execute this command.
`SET BAY BOOT ONCE [HDD | PXE | RBSU] <bay number> {[ , | - ] <bay number>}`	Sets the boot device to be used on the next boot of the bay(s) specified. This setting is only valid on present blades and is cleared if the blade is removed. This command requires BIOS version 06/15/02 or greater for the ProLiant BL10e server blade ROM.	Only enclosure and administrators may execute this command.

continued

Table 4-8: Functionality Exclusive to the Command Line Interface *continued*

Function	Description	Capability Exclusive to the Command Line Interface
Enclosure Management Commands, continued		
SHOW BAY LIST [ALL | <group name>]	Displays the assigned to group, remote console user, and server blade name for each bay in a particular group if a group name is specified or all bays if ALL is specified.	The command line displays the remote console user.
SHOW SYSLOG BAY <bay number>	Displays the syslog of a specified blade with 22 lines per screen Typing "q" quits the command; any other key shows the next screen if more information is available to display. The system log of the server blade is not stored between reboots, so the information only includes what has taken place since the last power on of the Integrated Administrator. Typing "c" displays the System Log continuously without page breaks.	All
ADD IPMANAGER <IP address>	Adds an IP address to the list of clients allowed to connect to Integrated Administrator.	Only enclosure administrators may execute this command.
DISABLE ALERTMAIL	Disables sending e-mail for Integrated Administrator alerts.	Only enclosure administrators may execute this command.
DISABLE IPSECURITY	Allows all clients to connect to Integrated Administrator.	Only enclosure administrators may execute this command.
DISABLE NTP	Disables automatic updates of the date and time to the Integrated Administrator.	Only enclosure administrators may execute this command.
ENABLE ALERTMAIL	Enables sending e-mail for Integrated Administrator alerts.	Only enclosure administrators may execute this command.
ENABLE IPSECURITY	Restricts clients from being able to connect to Integrated Administrator.	Only enclosure administrators may execute this command.

continued

Table 4-8: Functionality Exclusive to the Command Line Interface *continued*

Enclosure Management Commands, continued		
ENABLE NTP	Enables automatic time and date updates to Integrated Administrator.	Only enclosure administrators may execute this command.
REMOVE IPMANAGER <IP address>	Removes the IP address from the list of clients allowed to connect to Integrated Administrator.	Only enclosure administrators may execute this command.
SET ALERTMAIL [MAILBOX | SENDERDOMAIN | SMTPSERVER]	Sets the e-mail address of the alert recipient, the domain name, and the mail server address.	Only enclosure administrators may execute this command.
SET NTP [PRIMARY | SECONDARY | POLL]	Sets the IP address of the primary and secondary NTP servers. Also sets the frequency of the updates.	Only enclosure administrators may execute this command.
SHOW NETWORK	Displays the DHCP state, Dynamic DNS state, IP address, subnet mask, gateway address, primary and secondary DNS addresses, MAC address, HTTP and HTTPS server status, SNMP status, Secure Shell status, Telnet status, NTP status, NTP primary and secondary server address, NTP poll interval, NTP last update time, IP security configuration, AlertMail status, AlertMail mailbox, SMTP server address and sender domain of the enclosure.	Only enclosure administrators may execute this command.

5

Setting Up the System

This chapter explains the levels of user rights recognized by the Integrated Administrator and provides detailed procedures to configure the management functionalities provided by the Integrated Administrator.

- Customizing the enclosure settings
  - — Changing the Administrator password
  - — Modifying enclosure and rack names
  - — Modifying the asset tag number
  - — Modifying the date and time
- Setting up user accounts
  - — Adding a group
  - — Adding a user
- Enabling remote console sessions to server blades
- Setting up AlertMail
  - — Adding mailbox address
  - — Adding SMTP server address
  - — Adding Sender Domain
  - — Enabling AlertMail
  - — Disabling AlertMail

- Setting up IP Security
  - — Adding IP address
  - — Enabling IP Security
  - — Disabling IP Security
- Setting up Automatic Time Configuration (NTP)
  - — Adding primary NTP server
  - — Adding secondary NTP server
  - — Setting the poll interval
  - — Enabling NTP
  - — Disabling NTP
- Configuring SNMP support
  - — Entering a community string
  - — Modifying the system location
  - — Modifying the system contact information
  - — Adding trap targets
  - — Removing trap targets

For a detailed explanation of the command line conventions used in this document, see Appendix A, "Command Line Conventions."

These procedures are supported by the Web-based user interface and the CLI unless otherwise noted.

IMPORTANT: Most of these tasks are limited to a subset of users. For more information on who can perform each task, see the "User Permissions" section and the section describing that task in this chapter.

User Permissions

The group-centered approach of Integrated Administrator to user permissions facilitates the maintenance of user groups and groups of server blade bays. This approach operates according to the following principles:

- A server blade bay is assigned exclusively to one group only.
- A group can be assigned many server blade bays.
- A user can have various permission levels within any number of groups.
- Access to a server blade by users or groups depends on the rights assigned to the server blade bay in which the server blade is installed.

Use Table 5-1 to distinguish the various permission levels available from the ProLiant BL e-Class Integrated Administrator.

Table 5-1: Permission Levels of the ProLiant BL e-Class Integrated Administrator

Title	Account Type	Permissions	Description
Enclosure administrator	Administrator	View/Modify for all groups in the enclosure	Enclosure administrators may create, maintain, enable, and disable users and other enclosure administrators. Enclosure administrators may maintain server blade bay privileges, manage the enclosure, manage server blade bays, and create and maintain groups. One special enclosure administrator account (named "Administrator") cannot be deleted, disabled, or stripped of enclosure administrator permissions. No other enclosure administrator may change the password to this account. Enclosure administrators cannot disable or delete their own accounts.

continued

Table 5-1: Permission Levels of the ProLiant BL e-Class Integrated Administrator
continued

Title	Account Type	Permissions	Description
Group administrator	User	View/Modify	Group administrators may manage server blade bay data for groups in which they are administrators. Group administrators may view server blade bay data for groups in which they are members. Group administrators may modify their profile (not their privileges) and view enclosure data.
Group member	User	View	Group members may view server blade bay data for groups in which they are members. Group members may modify their profile (not their privileges) and view enclosure data.
User	User		Users may modify their profile (not their privileges) and view enclosure data.

Customizing the Enclosure Settings

IMPORTANT: Only enclosure administrators may execute these commands.

Changing the Administrator Password

To change the default Administrator password using the Web-based user interface:

1. Click the **Administration** tab.
2. Click **User List** in the side panel.
3. Click the **Administrator** user name in the user list.
4. Click **View/Modify User**. The **View/Modify User** screen displays.
5. Click **Change Password**.

6. Type in the new Administrator password in the **Password** and **Confirm password** fields.
7. Click **OK**.

To change the default Administrator password using the CLI, enter:

```
SET USER PASSWORD Administrator <new password>
```

IMPORTANT: The user name (Administrator) is case-sensitive. The <new password> must be 3-8 characters long and can include all printable characters.

Modifying Enclosure and Rack Names

To modify the enclosure name or rack name using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **Enclosure Information** in the left panel.
3. Click the **Enclosure Name** field of the **Status** area.
4. Type the enclosure name.
5. Click the **Rack Name** field of the **Status** area.
6. Type the rack name.

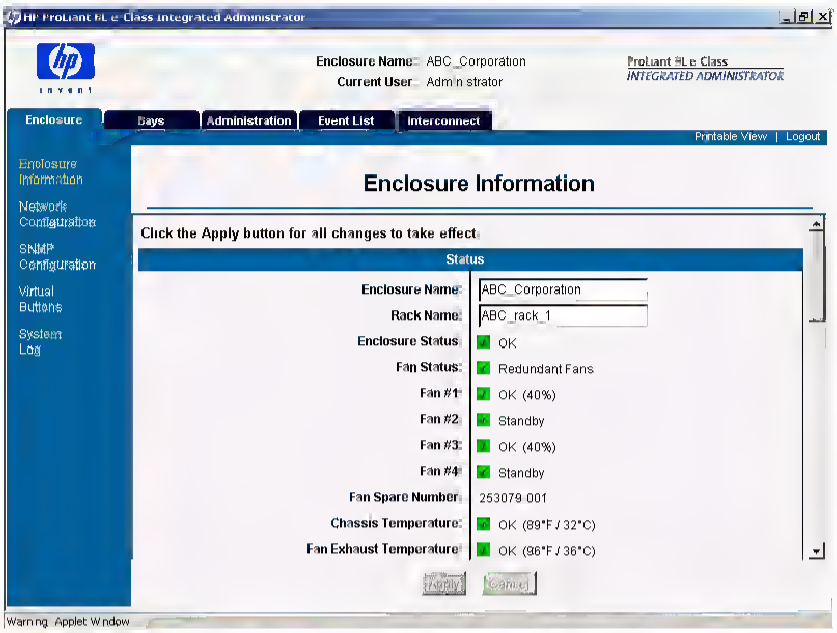


Figure 5-1: Setting the enclosure name and rack name

7. Click **Apply**.

To modify the enclosure name or rack name using the CLI, enter the following commands sequentially:

```
SET ENCLOSURE NAME <enclosure name>
```

IMPORTANT: The <enclosure name> must be 1-32 characters long and includes all alphanumeric, the dash, and the underscore characters.

The default enclosure name is IA-XXXXXXXXXXXX where XXXXXXXXXXXX is replaced with the actual MAC address.

```
SET RACK NAME <rack name>
```

IMPORTANT: The <rack name> must be a maximum of 32 characters long and includes all alphanumeric, dash, and underscore characters. The default rack name is "UnnamedRack."

Modifying the Asset Tag Number

To modify the asset tag number using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **Enclosure Information** in the left panel.
3. Scroll down to the **General** area.
4. Click the **Asset Tag** field.
5. Type the asset tag number.

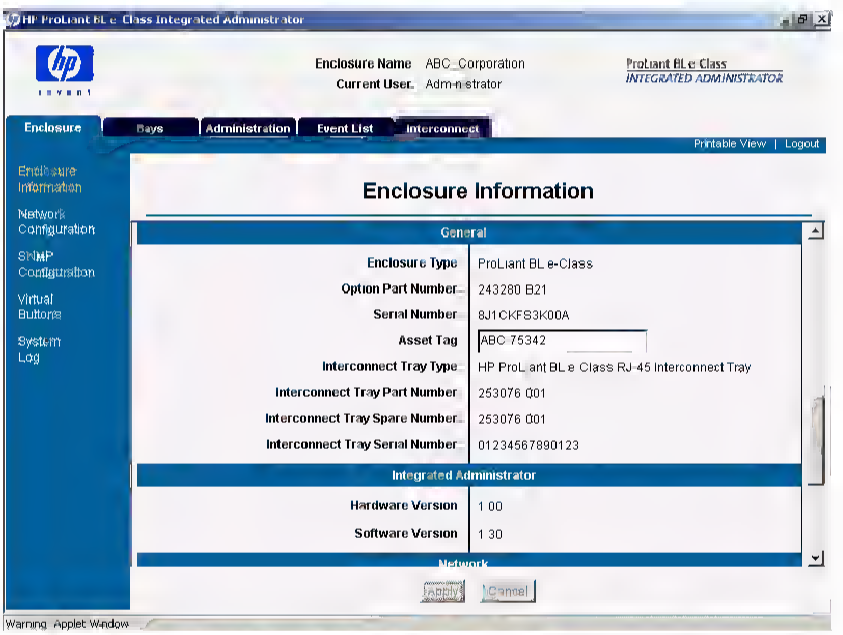


Figure 5-2: Setting the asset tag number

6. Click **Apply**.

To modify the asset tag number using the CLI, enter:

```
SET ENCLOSURE ASSET {TAG} <asset tag>
```

IMPORTANT: The <asset tag> must be 1-31 characters long and includes alphanumeric, dash, and underscore characters The default enclosure asset tag is blank.

Modifying the Date and Time

To modify the date and time settings using the Web-based user interface:

NOTE: On a Linux system, this information can only be modified using the CLI.

1. Click the **Enclosure** tab.
2. Click **Enclosure Information** in the left panel.
3. Scroll down to the **Date and Time** area.
4. Select the proper time zone from the pull-down list.
5. Click the **Date** or **Time** field.
6. Type the date or time.

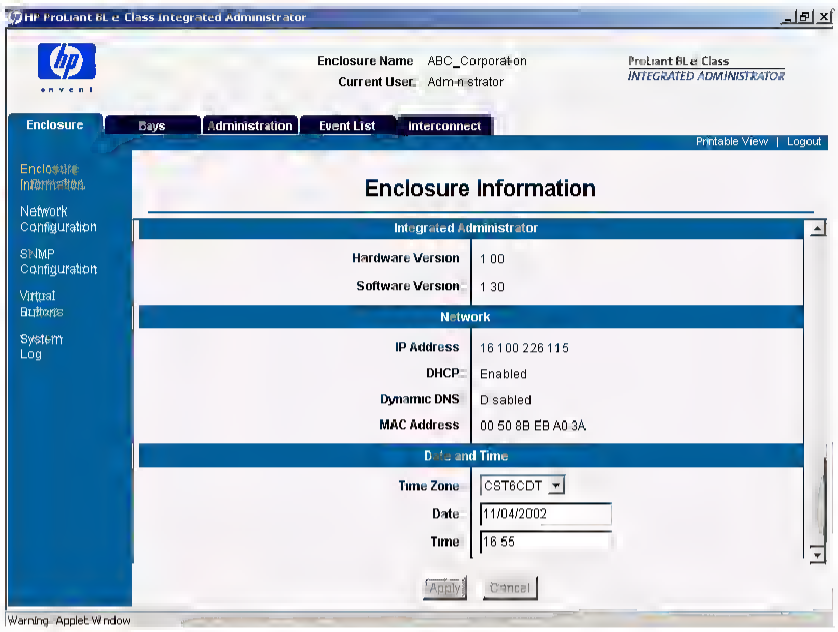


Figure 5-3: Setting the date and time

7. Click **Apply**.

To modify the date and time settings using the CLI, enter:

```
SET DATE MMDDhhmm{{CC}YY} {TZ}
```

where:

- *MM*: month
- *DD*: day
- *hh*: hour (24-hour time, an integer from 0-23)
- *mm*: minute
- *CC*: century
- *YY*: year
- *TZ*: timezone

IMPORTANT: If the time zone is left blank, the current time zone is left in effect. For a list of supported time zones, see Appendix F, "Time Zone Settings."

Setting Up User Accounts

IMPORTANT: Only enclosure administrators may perform this task.

The ProLiant BL e-Class Integrated Administrator enables you to manage server blade bays and administer users by organizing those server blade bays and users into groups.

This approach enables enclosure administrators, for example, to re-assign user permissions to groups of server blades en masse, instead of requiring enclosure administrators to modify permissions one user at a time.

Enclosure administrators assign users access rights to server blade bays through the following tasks:

- Adding groups with access to specific server blade bays in an enclosure
- Adding users with certain permissions within specific groups

Adding a Group

IMPORTANT: Restricted default names of group and user accounts (Administrator, switcha, and switchb) are not case-sensitive. Non-default group and user names are case-sensitive.

For more information on the Web-based user interface screens for this function, see the "Group List" section in Chapter 3, "Web-Based User Interface." For information on using the CLI, see the "User Account Commands" section in Chapter 4, "Command Line Interface."

To create a group using the Web-based user interface:

1. Click the **Administration** tab.
2. Click **Add Group in** the left panel.

3. Type the group name and description in the fields.
4. Select bays for the group by selecting the appropriate checkboxes.

IMPORTANT: If a server blade bay is gray, that server blade bay is inaccessible because it already belongs to another group.

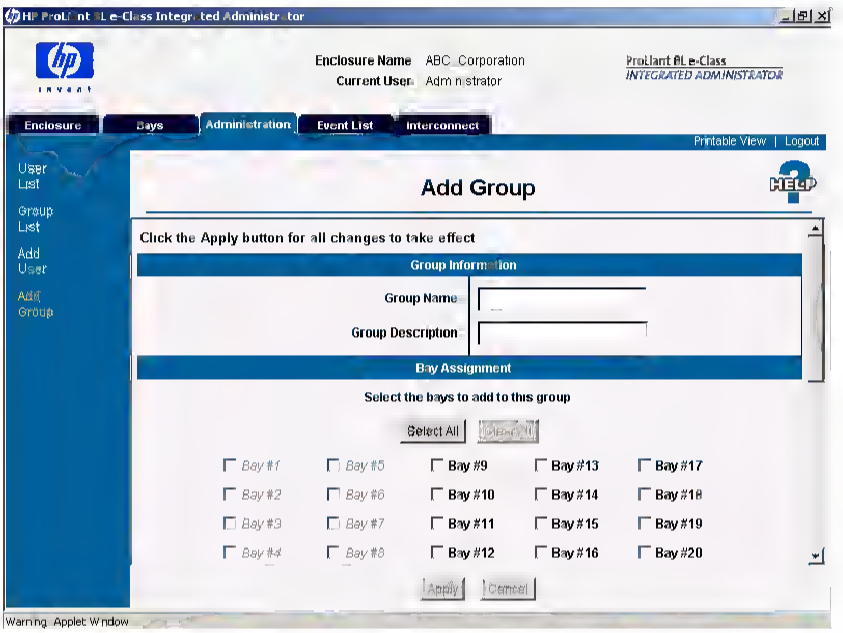


Figure 5-4: Setting a new group's name, description, and rights to server blade bays

5. To add existing users to this group:

   a. Select users in the **User Names** area.

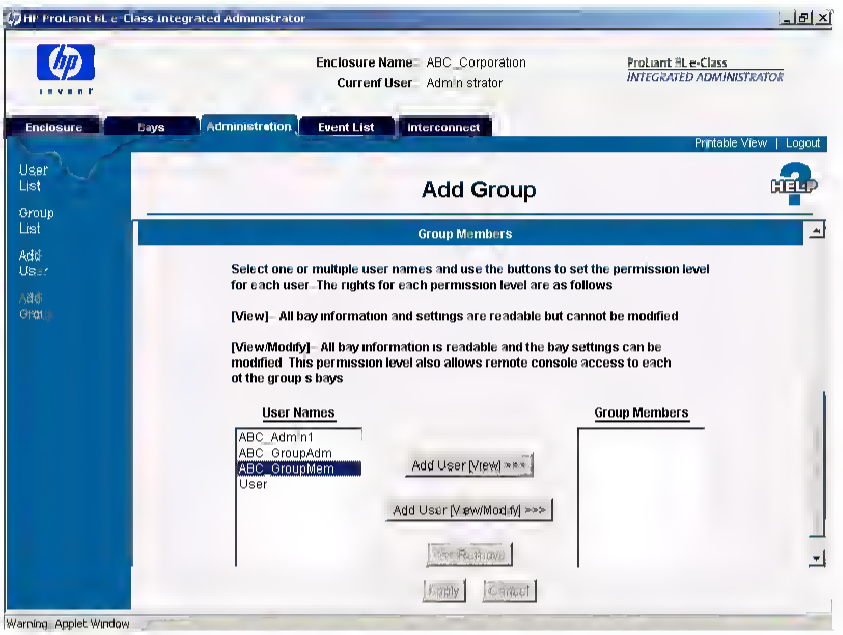

Enclosure Name: ABC_Corporation
Current User: Administrator
ProLiant BL e-Class
INTEGRATED ADMINISTRATOR
Enclosure
Bays
Administration
Event List
Interconnect
Printable View | Logout
User List
Group List
Add User
Add Group
Add Group
HELP
Group Members
Select one or multiple user names and use the buttons to set the permission level for each user. The rights for each permission level are as follows
[View] - All bay information and settings are readable but cannot be modified
[View/Modify] - All bay information is readable and the bay settings can be modified. This permission level also allows remote console access to each of the group's bays
User Names
ABC_Admin1
ABC_GroupAdm
ABC_GroupMem
User
Add User [View] >>>
Add User [View/Modify] >>>
Group Members
Apply
Cancel
Warning: Applet Window

Figure 5-5: Choosing an existing user to add to a new group (user highlighted)

b. Click **Add User [View]** or **Add User [View/Modify]**.

For more information on permission levels, see the "User Permissions" section in this chapter.

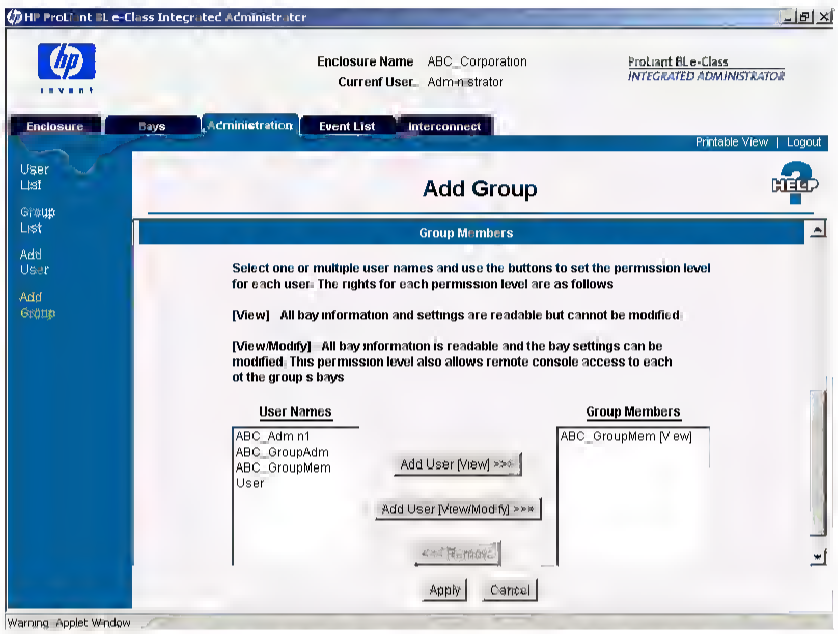


Figure 5-6: Giving an existing user View rights to a new group

6. Click **Apply**.

To create a group using the CLI, enter the following commands sequentially:

```
ADD GROUP <group name>
```

IMPORTANT: The <group name> must be unique to all other group names and user names and is case-sensitive. It must be 1-13 characters long and can include all alphanumeric characters, the dash, and the underscore.

```
SET GROUP {DESCRIPTION} <group name> <description>
```

IMPORTANT: The <description> must be 0-20 characters long and can include all alphanumeric characters, the dash, the underscore, and spaces.

```
ASSIGN BAY [ALL | <bay number> {[ , | - ]<bay number>}]
<group name>
ASSIGN USER <user name> <group name> {[VIEW | MODIFY]}
```

IMPORTANT: The <user name> and <group name> are case-sensitive. The "Administrator" account cannot be added to a group. The default setting is **View**.

Adding a User

IMPORTANT: Restricted default names of group and user accounts are not case-sensitive. Non-default group and user names are case-sensitive.

For information on permission levels, see the "User Permissions" section in this chapter.

To create a user using the Web-based user interface:

1. Click the **Administration** tab.
2. Click **Add User** in the left panel.

3. Type the user information in the appropriate field.

   For information on "Account Type," see the "User Permissions" section in this chapter.

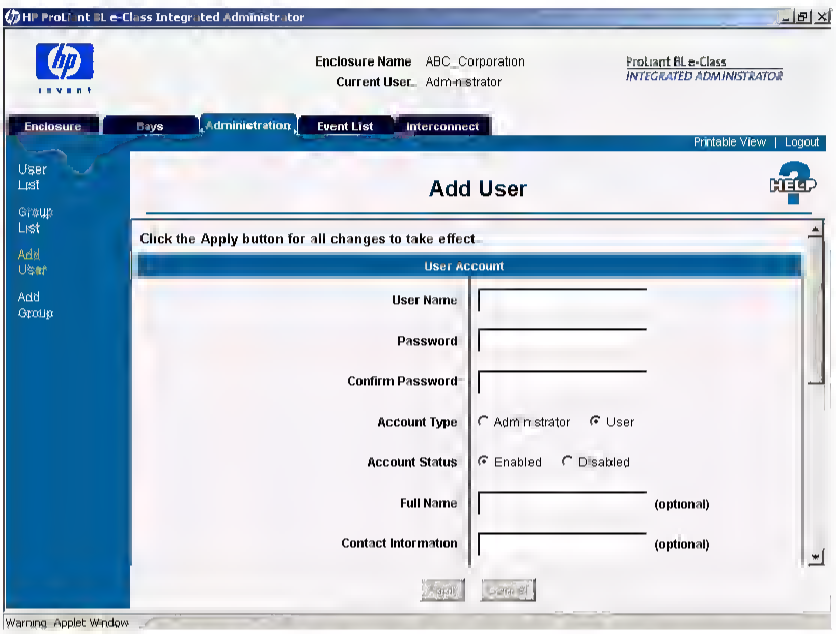


Figure 5-7: Setting a new user's name, password, rights, and ancillary information

NOTE: The **Account Type** setting determines whether the account holder has management permissions. The optional **Full Name** and **Contact Information** fields provide the account holder's name and a readily accessible means of contact in case of emergency.

4. To assign the user to an existing group:
   a. Select groups in the **Group Names** area.

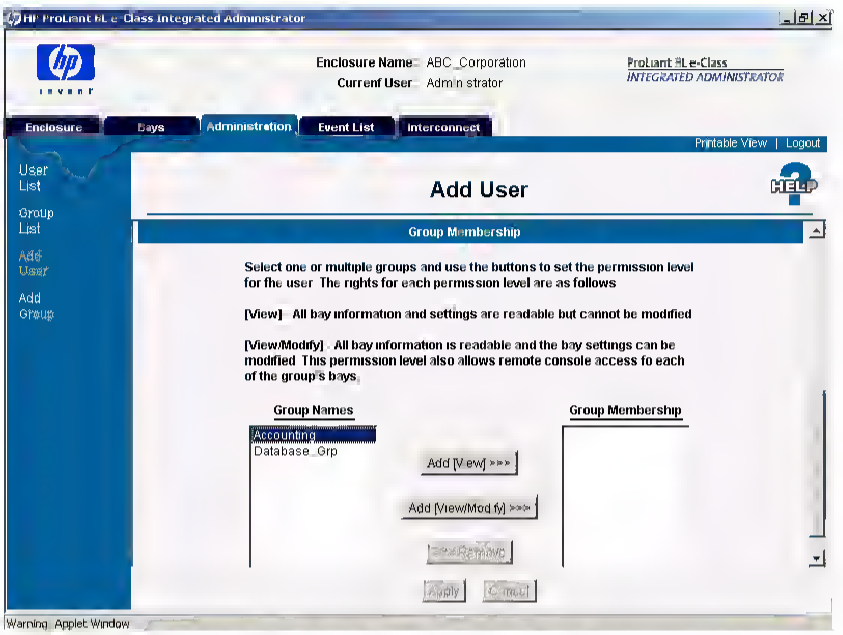

HP ProLiant BL e-Class Integrated Administrator
Enclosure Name: ABC_Corporation
Current User: Administrator
ProLiant BL e-Class
INTEGRATED ADMINISTRATOR
Enclosure
Bays
Administration
Event List
Interconnect
Printable View | Logout
User List
Group List
Add User
Add Group
Add User
HELP
Group Membership
Select one or multiple groups and use the buttons to set the permission level for the user. The rights for each permission level are as follows
[View] - All bay information and settings are readable but cannot be modified
[View/Modify] - All bay information is readable and the bay settings can be modified. This permission level also allows remote console access to each of the group's bays.
Group Names
Group Membership
Accounting
Database_Grp
Add [View] >>>
Add [View/Modify] >>>
Apply
Cancel
Warning: Applet Window

Figure 5-8: Choosing an existing group for the new user (group highlighted)

b. Click **Add User [View]** or **Add User [View/Modify]**.

For more information on permission levels, see the "User Permissions" section in this chapter.

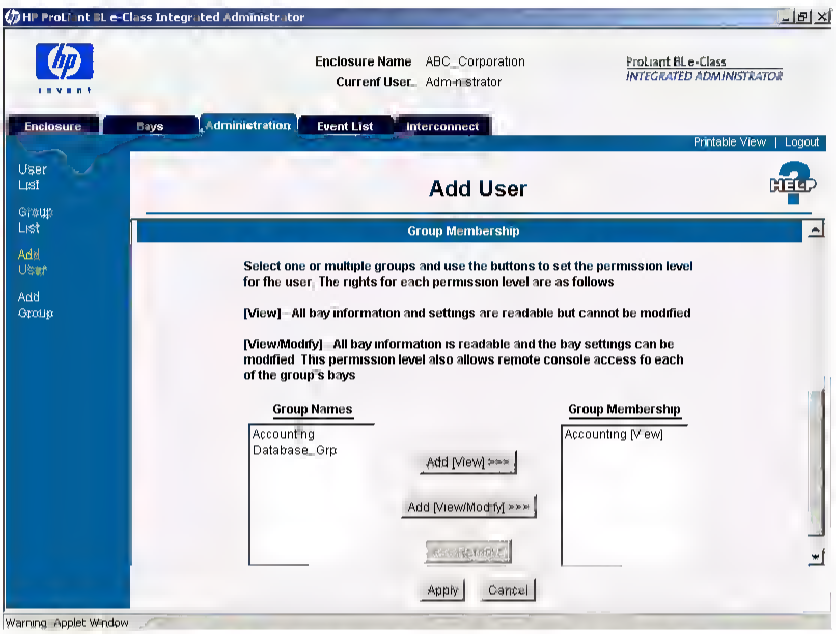


Figure 5-9: Giving a new user View rights to an existing group

5. Click **Apply**.

To add a user using the CLI, enter the following commands sequentially:

```
ADD USER <user name> {<password>}
```

IMPORTANT: The <user name> must be unique to all other user names and group names and is case-sensitive. It must be 1-13 characters long and can include all alphanumeric characters, the dash, and the underscore. The <password> must be 3-8 characters long and includes all printable characters.

```
ASSIGN ADMINISTRATOR {RIGHTS} <user name>
```

```
SET USER FULLNAME {<user name>} <full name>
```

IMPORTANT: The <full name> must be 0-20 characters long and can include all alphanumeric characters, the dash, the underscore, and spaces.

```
SET USER CONTACT {<user name>} <contact info>
```

IMPORTANT: The <contact info> must be 0-20 characters long and can include all alphanumeric characters, the dash, the underscore, and spaces.

```
ASSIGN USER <user name> <group name> {[VIEW | MODIFY]}
```

Enabling Remote Console Sessions to Server Blades

IMPORTANT: If a server blade is running the Windows 2000 operating system, only sequences that occur before the loading of the operating system are visible using Remote Console, unless the server blade is running the HP ProLiant Serial Console for Windows 2000 Server service.

To allow Remote Console access to a server blade, install the HP ProLiant Serial Console for Windows 2000 Server service, located at

www.compaq.com/support/files/server

The remote console feature of the Integrated Administrator enables a user to connect to the console (serial) connector of the server blade in order to access the ROM-Based Setup Utility (RBSU) and operating system of the server blade.

Accessing the RBSU of the server blade requires nothing more than connecting to the server blade. For detailed instruction to perform this task, see the "Accessing ROM-Based Setup Utility of a Server Blade" section in Chapter 6, "Performing Common Administrative Tasks."

Accessing the operation system for server blades running Linux requires preparatory steps that vary depending on whether you are using Linux Loader (LILO) or Grand Unified Boot Loader (GRUB).

To configure a server blade running Linux to use a serial console:

1. Attach the Diagnostic Adapter to the server blade you wish to configure.

NOTE: The Diagnostic Adapter ships with the enclosure.

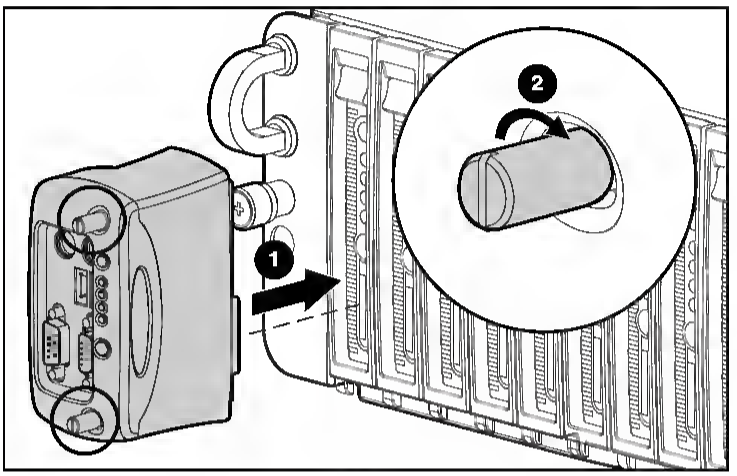


Figure 5-10: Attaching the Diagnostic Adapter

2. Connect a keyboard and monitor to the Diagnostic Adapter and log into the server blade as `root`.

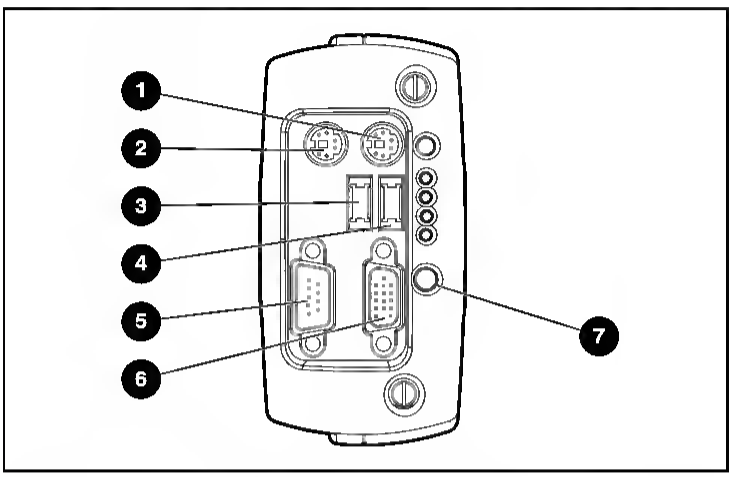


Figure 5-11: Components for configuring the Diagnostic Adapter

Table 5-2: Components for Configuring the Diagnostic Adapter

Item	Description
1	Keyboard connector
2	Mouse connector
3	USB 2 connector
4	USB 1 connector
5	Serial connector
6	Video connector
7	Power button

3. If your Linux server blade uses LILO:
   a. Remove the "message=" file specification from /etc/lilo.conf.

   IMPORTANT: Step a is necessary because the remote console of the Integrated Administrator is text-based, and the message file may be graphical.

   b. Add the following line to the 'linux' image specification in /etc/lilo.conf:

   ```
   append "console=tty0 console=ttyS0,115200"
   ```

CAUTION: Be sure the text in step a is indented in the file.

   c. Run /sbin/lilo to be sure that your changes take effect and continue with step 5.

4. If your Linux server blade uses GRUB, add the following line to the 'linux' image specification in /etc/grub.conf:

   ```
   append "console=tty0 console=ttyS0,115200"
   ```

CAUTION: Be sure the text in step 4 is indented in the specification.

5. Add the following line to the end of /etc/inittab:

   ```
   7:12345:respawn:/sbin/agetty 115200 ttyS0 vt100
   ```

6. Set "SAFE=yes" in the file /etc/sysconfig/kudzu.
7. Add the following line to /etc/securetty to allow root login on the serial console:

   ```
   ttyS0
   ```

After rebooting, the server blade is accessible remotely using the Integrated Administrator.

Setting Up AlertMail

AlertMail enables users to receive system events by e-mail instead of using SNMP traps. AlertMail is completely independent from SNMP and both can be enabled at the same time. AlertMail uses standard SMTP commands to communicate with an SMTP capable mail server.

Table 5-3: AlertMail Commands

Function	Command
Add an e-mail address using command line interface	SET ALERTMAIL MAILBOX <e-mail address>
Add an SMTP server address	SET ALERTMAIL SMTPSERVER <ip address>
Set the sender domain*	SET ALERTMAIL SENDERDOMAIN <domain name>
Enable AlertMail	ENABLE ALERTMAIL
Disable AlertMail	DISABLE ALERTMAIL

* For security reasons, some SMTP servers will only forward mail if the sender's domain is set properly. You may need to set this parameter to match the network domain.

E-mail Alerts

AlertMail, if enabled, will send out alerts by e-mail for the following events:

- Enclosure boot message
- IA reboot message
- Fan status change
- Fan inserted
- Fan removed
- Enclosure thermal status change

- Power supply status change
- Power supply inserted
- Power supply removed
- Power subsystem redundancy change
- Blade inserted
- Blade removed
- Blade status change
- Blade thermal change
- Blade fault

NOTE: If the enclosure has a switch installed, it can take up to 60 seconds before the system will send out an AlertMail after a system boot up. Events generated within this period of time will be sent out when the switch has come online.

All e-mails have the following header:

Subject: HP AlertMail-SEQ: <SEVERITY> SUBJECT

Date: Date in standard format

From: Enclosure ENCLOSURE-NAME <enclosure-name@domain>

To: RECEIVER MAILBOX

Where SEVERITY is one of the following:

- Highest
- # CRITICAL
- # WARNING
- # NOTICE
- # INFO
- Lowest

Example e-mail:

----SAMPLE START----

Subject: HP AlertMail-010: (CRITICAL) Power Supply #1: Failed

Date: Wed, 23 Apr 2003 15:02:22 +0200

From: Enclosure 1A-00508BEBA571 <1A-00508BEBA571@hp.com>

To: user@userdomain

X-OS: HP Integrated Administrator

X-Priority: 1

Content-Type: text/plain; charset=us-ascii

EVENT (26 May 07:09): Power Supply #1 Status has changed to: Failed

Enclosure, IA-00508BEBA571, has detected that a power supply in bay 1 has changed from status OK to Failed.

The power supply should be replaced with the appropriate spare part. You can ensure that the center wall assembly is operating correctly by swapping the two power supplies. Make sure that there are no bent pins on the power supply connectors before reinserting and that each power supply is fully seated.

An amber LED on the power supply indicates either an over-voltage, over-temperature, or loss of AC power has occurred. A blinking LED on the power supply indicates a current limit condition.

Enclosure Status: Degraded

Enclosure Management URL: <https://16.181.75.213/>

- PLEASE DO NOT REPLY TO THIS EMAIL –

----SAMPLE END----

Setting Up IP Security

IP security allows an administrator to define a set of IP addresses that are the only ones allowed to connect to the services provided (SSH, HTTP, TELNET, SNMP). This means that an administrator can make sure only a certain set of machines have access to Integrated Administrator. A maximum of five IP addresses can be entered.

Table 5-4: IP Security Commands

Function	Command
Add an IP address	ADD IPMANAGER <ip address>
Remove an IP address	REMOVE IPMANAGER <ip address>
Enable IP Security	ENABLE IPSECURITY
Disable IP Security	DISABLE IPSECURITY

Setting Up Automatic Time Configuration (NTP)

Automatic time configuration allows the Integrated Administrator to synchronize its date and time with a server supporting the Network Time Protocol (NTP).

Table 5-5: Automatic Time Configuration Commands

Set the NTP poll interval*	SET NTP POLL <seconds>
Set the primary NTP server	SET NTP PRIMARY <ip address>
Set the secondary NTP server	SET NTP SECONDARY <ip address>
Disable the secondary NTP server	SET NTP SECONDARY NONE
Enable NTP	ENABLE NTP
Disable NTP	DISABLE NTP

* If an NTP poll interval is not set, it will default to 720 seconds. The minimum time interval is 60 seconds and the maximum is 9999 seconds.

Configuring SNMP Support

IMPORTANT: Only enclosure administrators may execute these tasks.

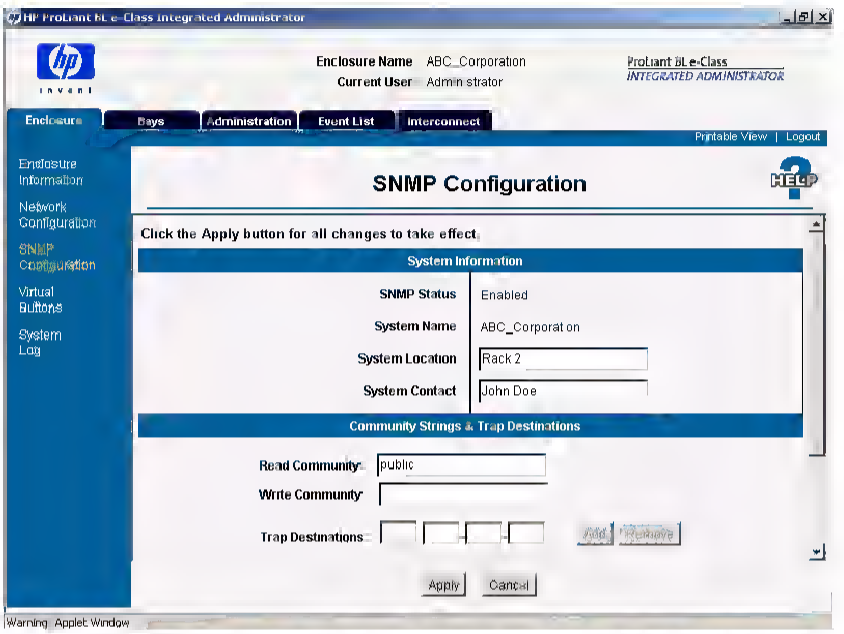


Figure 5-12: Setting a community string, trap target destinations, or system location and contact information

Entering a Community String

To enter a read community or write community string using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **SNMP Configuration** in the left panel.
3. Click the **Read Community** or **Write Community** field.

4. Type the string.

   IMPORTANT: Entering a blank string into the **Read Community** field sets the Read Community to "public." Entering a blank string into the **Write Community** field disables the SNMP set commands.

5. Click **Apply**.

To enter a read community or write community string using the CLI, enter:

```
SET SNMP COMMUNITY [READ | WRITE] <community name>
```

The write <community name> must be 0-20 characters long and the read <community name> must be 1-20 characters long. Both community names support all alphanumeric characters, the underscore, and the dash characters.

The default read community name is "public," and the default write community name is blank.

Modifying the System Location

IMPORTANT: The SNMP protocol can be disabled in the Network Configuration area of the Web-based user interface. See the "SNMP Configuration" section in Chapter 3, "Web-Based User Interface."

To modify the system location information using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **SNMP Configuration** in the left panel.
3. Set the cursor in the **System Location** field and type the appropriate information.
4. Click **Apply**.

To modify the system location information using the CLI, enter:

```
SET SNMP LOCATION <location>
```

The <location> field must be 0-20 characters long and supports all the alphanumeric characters, the underscore, the dash, and spaces with quotes.

Modifying the System Contact Information

To modify the system contact information using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **SNMP Configuration** in the left panel.
3. Set the cursor in the **System Contact** field and type the appropriate information.
4. Click **Apply**.

To modify the system contact information using the CLI, enter:

```
SET SNMP CONTACT <contact>
```

The <contact> field must be 0-20 characters long and supports all the alphanumeric characters, the underscore, the dash, and spaces with quotes.

Adding Trap Targets

To add a trap target using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **SNMP Configuration** in the left panel.
3. Type the IP address in the appropriate field of the **SNMP** area.
4. Click **Add**.
5. Click **Apply**.

To add a trap target using the CLI, enter:

```
ADD SNMP TRAPRECEIVER <IP address>
```

The <IP address> must be in the form ###.###.###.###, where ### ranges from 0 to 255.

The Integrated Administrator only supports v1 traps and directs the traps to SNMP port 162 by default. A maximum of eight IP addresses can be added to receive SNMP traps.

Removing Trap Targets

To remove a trap target list using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **SNMP Configuration** in the left panel.
3. Type the list name in the appropriate field of the **SNMP** area.
4. Click **Remove**.
5. Click **Apply**.

To add or remove a trap target list using the CLI, enter:

```
REMOVE SNMP TRAPRECEIVER <IP address>
```

The <IP address> must be in the form ###.###.###.###, where ### ranges from 0 to 255.

6

Performing Common Administrative Tasks

This chapter explains the Integrated Administrator management functionalities:

- Managing server blade bays
  - — Opening a remote console session to a server blade
  - — Accessing ROM-Based Setup Utility for a server blade
  - — Reviewing the activity for a server blade
  - — Powering off the server blade

CAUTION: Without the server blade health driver, the Integrated Administrator cannot gracefully shutdown a server blade.

  - — Identifying a server blade using the Unit Identification LED
- Managing the enclosure
  - — Reviewing the activity for the enclosure
  - — Identifying the enclosure using the Unit Identification LED
  - — Generating an enclosure summary
  - — Identifying problem components
- Managing users
  - — Modifying a user's rights to server blade bays
  - — Disabling and deleting user accounts

Managing Server Blade Bays

Opening a Remote Console Session to a Server Blade

IMPORTANT: If a server blade is running the Windows 2000 operating system, only sequences that occur before the loading of the operating system are visible using Remote Console, unless the server blade is running the HP ProLiant Serial Console for Windows 2000 Server service.

To allow Remote Console access to a server blade, install the HP ProLiant Serial Console for Windows 2000 Server service, located at

www.compaq.com/support/files/server

IMPORTANT: Enclosure administrators and group administrators with access to the bay can click the **Remote Console** button to open a remote text-based console to the server blade in the bay.

To access the remote console using the Web-based user interface:

1. Click the **Bays** tab.
2. Click **Bay List** in the left panel.

3. Select the server blade from the blade list.

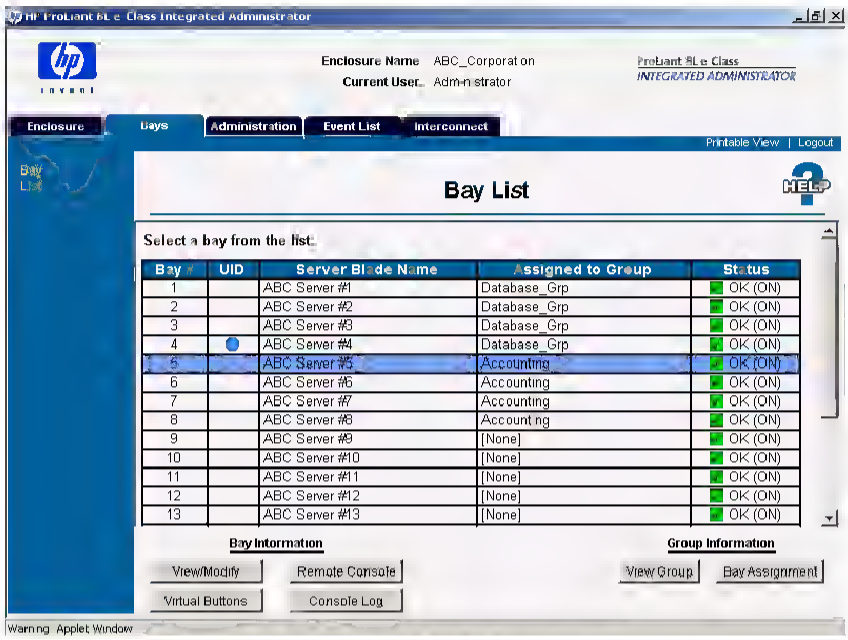

HP ProLiant BL e Class Integrated Administrator
Enclosure Name ABC_Corporation
Current User Administrator
ProLiant BL e Class
INTEGRATED ADMINISTRATOR
Enclosure
Bays
Administration
Event List
Interconnect
Printable View | Logout
Bay List
HELP
Bay List
Select a bay from the list:
Bay # | UID | Server Blade Name | Assigned to Group | Status
1 | ABC Server #1 | Database_Grp | OK (ON)
2 | ABC Server #2 | Database_Grp | OK (ON)
3 | ABC Server #3 | Database_Grp | OK (ON)
4 | ABC Server #4 | Database_Grp | OK (ON)
5 | ABC Server #5 | Accounting | OK (ON)
6 | ABC Server #6 | Accounting | OK (ON)
7 | ABC Server #7 | Accounting | OK (ON)
8 | ABC Server #8 | Accounting | OK (ON)
9 | ABC Server #9 | [None] | OK (ON)
10 | ABC Server #10 | [None] | OK (ON)
11 | ABC Server #11 | [None] | OK (ON)
12 | ABC Server #12 | [None] | OK (ON)
13 | ABC Server #13 | [None] | OK (ON)
Bay Information
View/Modify
Remote Console
Virtual Buttons
Console Log
Group Information
View Group
Bay Assignment
Warning: Applet Window

Figure 6-1: Choosing a server blade bay (server blade bay 5 highlighted)

4. Click **Remote Console**. The **Remote Console** screen displays.
5. Click **Remote Console**. This action opens a new window that enables you to connect to the server blade terminal interface.

To access the remote console using the CLI, enter:

```
CONNECT BAY <bay number>
```

IMPORTANT: A server blade can only support one remote console session at a time.

Accessing the ROM-Based Setup Utility for a Server Blade

IMPORTANT: Enclosure administrators and group administrators with access to the bay can select the **Remote Console** button to open a remote text-based console to the server blade in the bay.

To access the ROM-Based Setup Utility (RBSU) for a server blade using the Web-based user interface:

1. For server blades running the Linux operating system, be sure the server blades have been configured to support Remote Console sessions. See the "Opening a Remote Console Session to a Server Blade" section in this chapter.
2. Click the **Bays** tab.
3. Click **Bay List** in the left panel.
4. Select the bay from the bay list.
5. Click **Remote Console** at the bottom of the screen.
6. Click **Remote Console** from the **Remote Console** screen.
7. If the server blade is running the Windows 2000 operating system:
   a. Return to the Web-based user interface and click **Virtual Buttons** in the left panel.

CAUTION: Without the server blade health driver, the Integrated Administrator cannot reboot a server blade.

   b. If the server blade is off, select **Power On** at the bottom of the screen; otherwise, select **Reboot** at the bottom of the screen.
   c. Click **Apply** and return to the remote console session.
8. If the server blade is running the Linux operating system:
   a. Press the **Enter** key to get a prompt.
   b. Reboot the server blade.

9. When prompted to press the **F9** key for ROM-Based Setup Utility:
   a. Press the **Esc** key.
   b. Press the **9** key.
10. To exit RBSU:
   a. Press the **Esc** key.
   b. When prompted to press **F10**, press the **Esc** key and the **0** key to confirm.
11. To close the remote console session:
   a. Press the **Ctrl-_** keys.
   b. Press the **D** key.

To access the RBSU for a server blade using the command line interface:

CAUTION: Without the server blade health driver, the Integrated Administrator cannot reboot a server blade.

1. If the server blade is running the Windows 2000 operating system, reboot the server blade by entering the following commands sequentially:

   ```
   REBOOT BAY <bay number>
   Yes
   ```

2. Connect to the server blade by observing its bay number and entering:

   ```
   CONNECT BAY <bay number>
   ```

3. If the server blade is running the Linux operating system reboot the server blade:
   a. Press the **Enter** key to get a prompt.
   b. Enter your user name and password.
   c. Enter:

   ```
   REBOOT BAY <bay number> RBSU
   ```

4. When prompted to press the **F9** key for ROM-Based Setup Utility:
   a. Press the **Esc** key.
   b. Press the **9** key.
5. To exit RBSU:
   a. Press the **Esc** key.
   b. When prompted to press **F10**, press the **Esc** key and the **0** key to confirm.
6. To close the remote console session:
   a. Press the **Ctrl-_** keys.
   b. Press the **D** key.

Reviewing Activity for a Server Blade

IMPORTANT: This task can only be performed for a given server blade bay by enclosure administrators, group administrators, and group members with access rights to the server blade bay.

To access the console log for a server blade using the Web-based user interface:

1. Click the **Bays** tab.
2. Click **Bay List** in the left panel.
3. Choose the bay from the **Bay list**.
4. Click **Console Log** under **Bay Information**.

To view the system log for a server blade using the CLI, enter:

```
SHOW SYSLOG BAY <bay number>
```

IMPORTANT: Entering "q" quits the command. Typing any other key shows the next screen if more information is available to display. The system log of the server blade is not stored between reboots, so the information only includes what has taken place since the last power-on of the Integrated Administrator.

Powering Off the Server Blade

CAUTION: Without the server blade health driver or an ACPI-compliant operating system, the Integrated Administrator cannot gracefully shutdown a server blade. This condition may result in the permanent loss of critical data.

CAUTION: Rebooting or powering off the server blade removes all power from the server blade and ends all open sessions.

IMPORTANT: This task can only be performed for a given server blade bay by enclosure administrators and group administrators with access rights to the server blade bay.

To reboot or power off the server blade using the Web-based user interface:

1. Click the **Bays** tab.
2. Click **Bay List** in the left panel.
3. Click the server blade whose power state you wish to modify.
4. Click **Virtual Buttons** at the bottom of the screen.

5. Click **Reboot**, **Power Off** or **Power Off Immediately**.

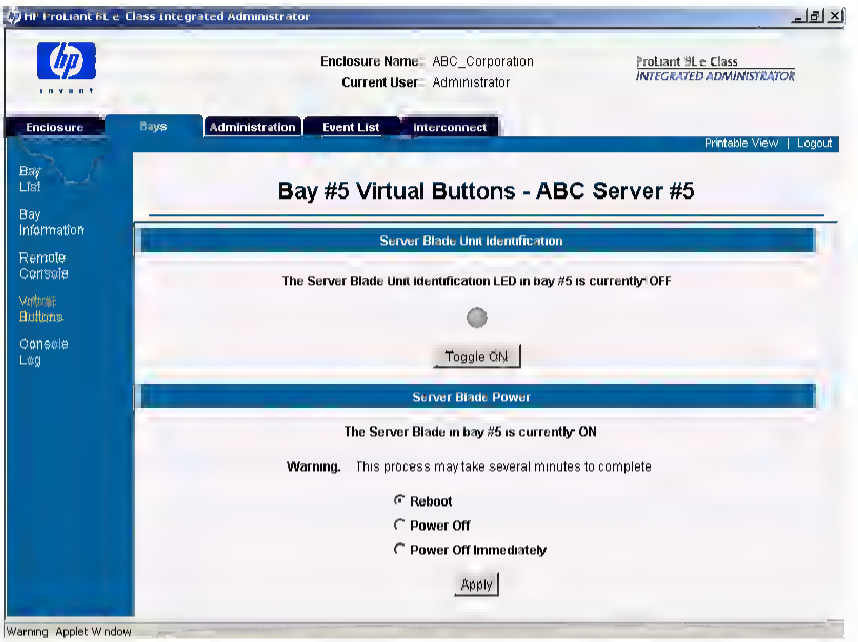


Figure 6-2: Managing server blade power

6. Click **Apply**.

   When the server blade power is off, the **Power Off** button text becomes **Power On**.

To reboot the server blade using the CLI, enter:

```
REBOOT BAY <bay number> {[ , | - ] <bay number>} {FORCE}
{[PXE | HDD | RBSU]}
```

NOTE: This command sends a request to the server blade in a given bay to perform a graceful shutdown and then reboots the server blade.

To power off the server blade (immediately or otherwise) using the CLI, enter:

```
POWEROFF BAY <bay number> {[ , | - ] <bay number>} {FORCE}
```

IMPORTANT: If the FORCE argument is invoked, the server blade powers down immediately and could lose data or become unstable.

Identifying a Server Blade Using the Unit Identification LED

IMPORTANT: This task can only be performed for a given server blade bay by enclosure administrators and group administrators with access rights to the server blade bay.

The virtual button for the Unit Identification LED of the server blade physically changes the state of the Unit Identification LED on the front panel of the server blade from off to on, or vice-versa. The Unit Identification LED illuminates bright blue and is designed to help a technician quickly identify a specific server blade in the data center.

To change the state of a Unit Identification LED of for a server blade using the Web-based user interface:

1. Click the **Bays** tab.
2. Click **Bay List** in the left panel.
3. Click the server blade whose Unit Identification LED you wish to toggle.
4. Click **Virtual Buttons** at the bottom of the screen.

5. Click **Toggle ON** or **Toggle OFF** depending on the current state of the Unit Identification LED for the server blade.

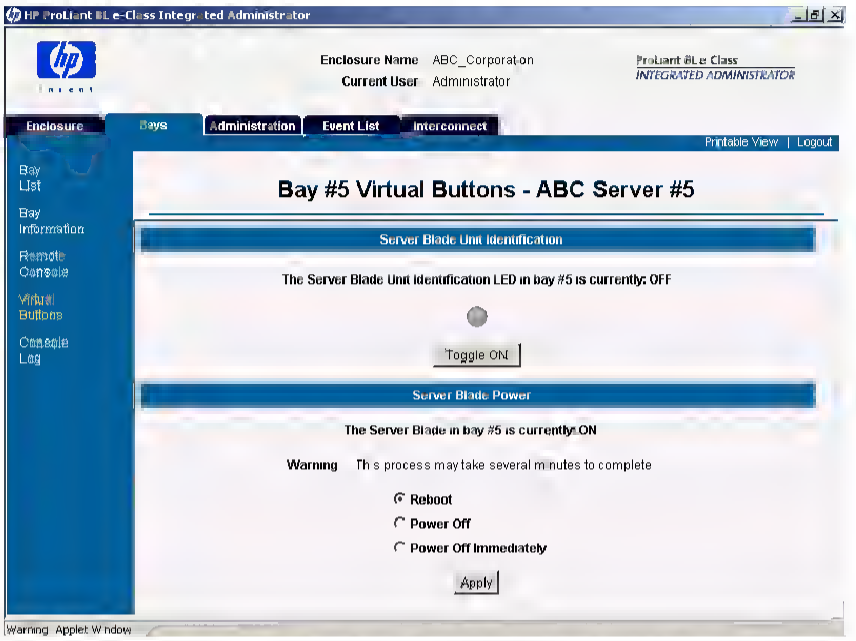


Figure 6-3: Accessing the Unit Identification LED button for a server blade (shown in the off state)

To change the state of the Unit Identification LED for a server blade using the CLI, enter:

```
SET BAY UID <bay number> {[ , | - ] <bay number>} [ON | OFF]
```

Managing the Enclosure

Reviewing the Activity of the Enclosure

The system log of the Integrated Administrator is a chronology of system activities, such as user logins, enclosure shutdowns, and system failures. The system log also displays warnings and errors that occur in the ProLiant BL e-Class system, including:

- User account modifications
- Group modifications
- Bay assignment modifications
- Valid and invalid login attempts
- System failures
- System status changes
- Blade insertion and removals
- DHCP, Dynamic DNS, and WINS messages
- Updates to the Integrated Administrator's firmware

Enclosure administrators can view events in the enclosure by accessing the System Log. In contrast to the Event List, no other users can access the System Log. For more information on how the Event List differs from the System Log, see the "Identifying Problem Components" section in this chapter.

To view the System Log using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **System Log** in the left panel.

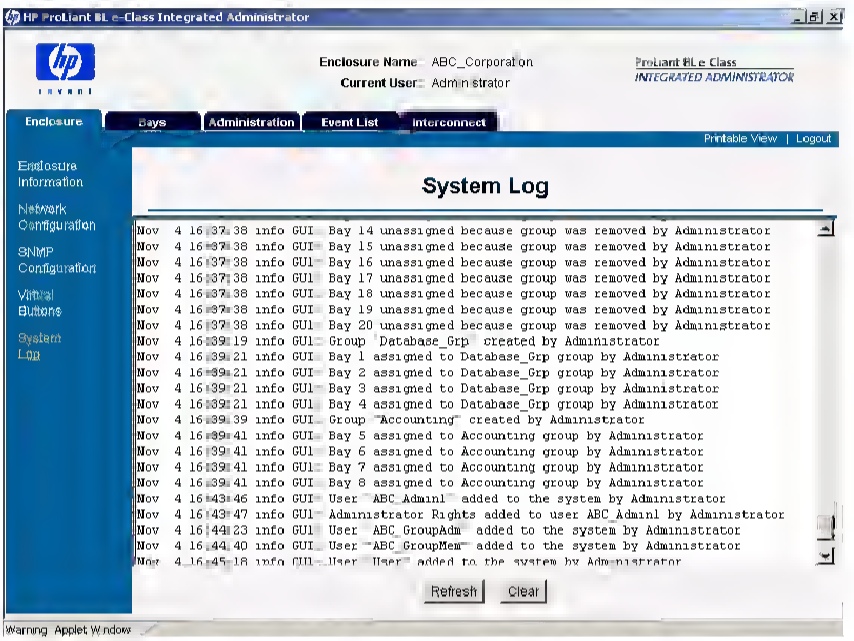

HP ProLiant BL e-Class Integrated Administrator
Enclosure Name: ABC_Corporation
Current User: Administrator
ProLiant BL e Class
INTEGRATED ADMINISTRATOR
Enclosure
Bays
Administration
Event List
Interconnect
Printable View | Logout
Enclosure Information
Network Configuration
SNMP Configuration
Virtual Buttons
System Log
System Log
Nov 4 16:37:38 info GUI Bay 14 unassigned because group was removed by Administrator
Nov 4 16:37:38 info GUI Bay 15 unassigned because group was removed by Administrator
Nov 4 16:37:38 info GUI Bay 16 unassigned because group was removed by Administrator
Nov 4 16:37:38 info GUI Bay 17 unassigned because group was removed by Administrator
Nov 4 16:37:38 info GUI Bay 18 unassigned because group was removed by Administrator
Nov 4 16:37:38 info GUI Bay 19 unassigned because group was removed by Administrator
Nov 4 16:37:38 info GUI Bay 20 unassigned because group was removed by Administrator
Nov 4 16:39:19 info GUI Group "Database_Grp" created by Administrator
Nov 4 16:39:21 info GUI Bay 1 assigned to Database_Grp group by Administrator
Nov 4 16:39:21 info GUI Bay 2 assigned to Database_Grp group by Administrator
Nov 4 16:39:21 info GUI Bay 3 assigned to Database_Grp group by Administrator
Nov 4 16:39:21 info GUI Bay 4 assigned to Database_Grp group by Administrator
Nov 4 16:39:39 info GUI Group "Accounting" created by Administrator
Nov 4 16:39:41 info GUI Bay 5 assigned to Accounting group by Administrator
Nov 4 16:39:41 info GUI Bay 6 assigned to Accounting group by Administrator
Nov 4 16:39:41 info GUI Bay 7 assigned to Accounting group by Administrator
Nov 4 16:39:41 info GUI Bay 8 assigned to Accounting group by Administrator
Nov 4 16:43:46 info GUI User "ABC_Admin1" added to the system by Administrator
Nov 4 16:43:47 info GUI Administrator Rights added to user ABC_Admin1 by Administrator
Nov 4 16:44:23 info GUI User "ABC_GroupAdm" added to the system by Administrator
Nov 4 16:44:40 info GUI User "ABC_GroupMem" added to the system by Administrator
Nov 4 16:45:18 info GUI User "User" added to the system by Administrator
Refresh
Clear
Warning: Applet Window

Figure 6-4: Accessing the enclosure's system log

3. To update the System Log, click **Refresh**.
4. To clear the System Log, click **Clear Log**. The Integrated Administrator prompts you to confirm this decision.

To view the System Log of the enclosure using the CLI, enter:

```
SHOW SYSLOG ENCLOSURE
```

IMPORTANT: Only enclosure administrators can execute this command.

Identifying the Enclosure Using the Unit Identification LED

The virtual button for the Unit Identification LED of an enclosure physically changes the state of the Unit Identification LED on the rear panel of the enclosure from Off to On, or vice-versa. The Unit Identification LED illuminates bright blue and is designed to help a technician quickly identify a specific enclosure in the data center.

To change the state of the Unit Identification LED of the enclosure using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **Virtual Buttons** in the left panel.
3. Click **Toggle ON** or **Toggle OFF** depending on the current state of the Unit Identification LED for the enclosure.

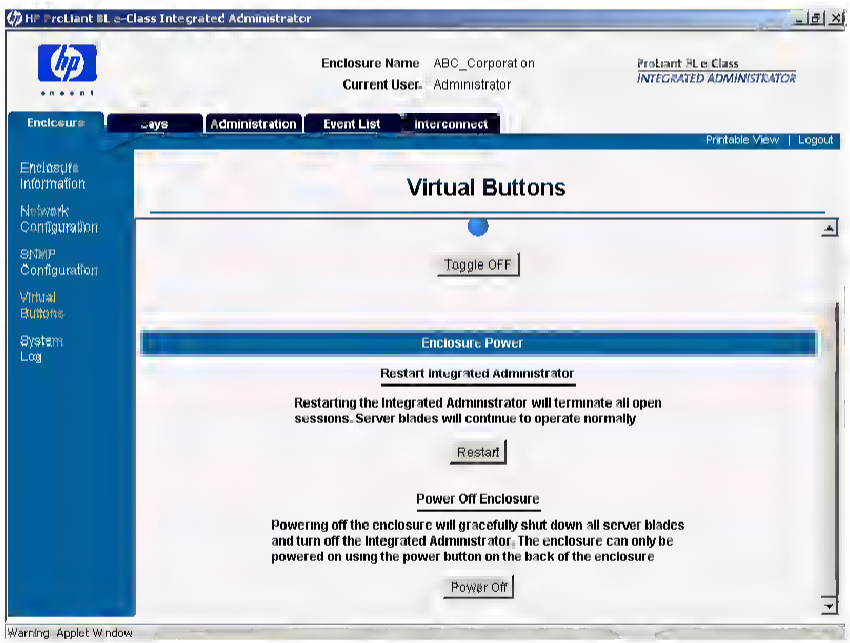

Enclosure Name ABC_Corporat on
Current User: Administrator
ProLiant BL e-Class
INTEGRATED ADMINISTRATOR
Enclosure
Administration
Event List
Interconnect
Printable View | Logout
Enclosure Information
Network Configuration
SNMP Configuration
Virtual Buttons
System Log
Virtual Buttons
Toggle OFF
Enclosure Power
Restart Integrated Administrator
Restarting the Integrated Administrator will terminate all open sessions. Server blades will continue to operate normally
Restart
Power Off Enclosure
Powering off the enclosure will gracefully shut down all server blades and turn off the Integrated Administrator. The enclosure can only be powered on using the power button on the back of the enclosure
Power Off
Warning: Applet Window

Figure 6-5: Accessing the Unit Identification LED button for the enclosure (shown in the on state)

To change the state of the Unit Identification LED for the enclosure using the CLI, enter:

```
SET ENCLOSURE UID [ON | OFF]
```

IMPORTANT: Only enclosure administrators may execute this command.

Generating an Enclosure Summary

You can generate a printable synopsis of all the data for the enclosure including the enclosure name and type; the part, serial, and asset tag numbers of the enclosure; the software and hardware versions of the Integrated Administrator; the MAC address of the Integrated Administrator; and the type, part number, and serial number of the interconnect tray.

To generate a printable synopsis of all the data for the enclosure using the Web-based user interface, click **Printable View** in the top panel. The Web-based user interface opens a new window that shows all enclosure information, which you can copy and paste into a printable file.

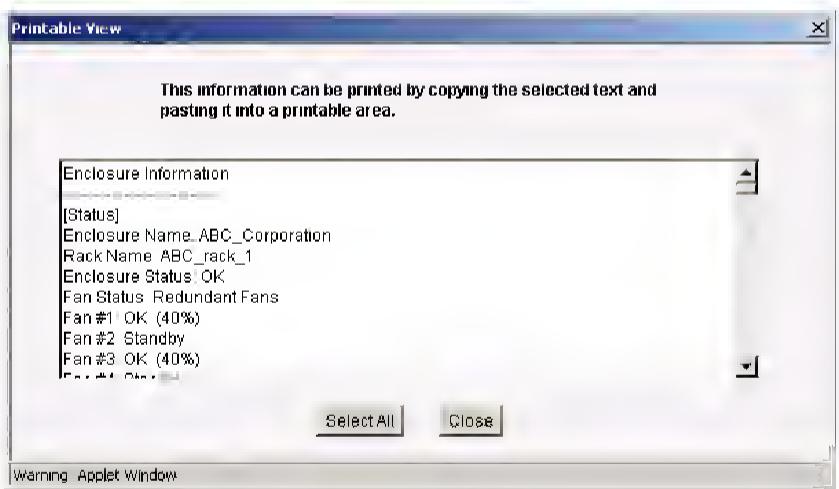


Figure 6-6: Generating an enclosure summary

To obtain the enclosure information using the CLI, enter the following commands as needed:

```
SHOW ENCLOSURE FAN [<fan number> | ALL]
```

IMPORTANT: This command displays the status, redundancy, partner, speed, and part number for one or all fans in the enclosure.

```
SHOW ENCLOSURE INFO
```

IMPORTANT: This command displays the enclosure name and enclosure type; the software and hardware version of the Integrated Administrator; the part number, serial number, and asset tag number of the enclosure; the MAC address of the Integrated Administrator; and the type, part number, and serial number of the interconnect tray.

```
SHOW ENCLOSURE POWERSUPPLY [<power supply number> | ALL]
```

IMPORTANT: This command displays the status, AC input status, capacity, input voltage range #1 (Volts), input voltage range #2 (Volts), input frequency range (Hz), part number, serial number, and hardware revision for one or all power supplies in the enclosure.

```
SHOW ENCLOSURE STATUS
```

IMPORTANT: This command displays the status of enclosure health, Integrated Administrator health, and the Unit Identification LED under the heading "enclosure status," and displays the status and capacity of the power supplies of the enclosure under the heading "power status."

```
SHOW ENCLOSURE TEMP
```

IMPORTANT: This command displays the location, status (OK, warm, degraded, or failed), and temperature (degrees Fahrenheit and Celsius) for all the temperature sensors of the enclosure.

Identifying Problem Components

The Integrated Administrator alerts you to problem conditions or failed components in the enclosure, such as:

- A fan
- A power supply
- A server blade
- Over-temperature conditions

If the enclosure enters a degraded state at any time, the Web-based user interface of the Integrated Administrator alerts the user with icons along the top of the deck panel.

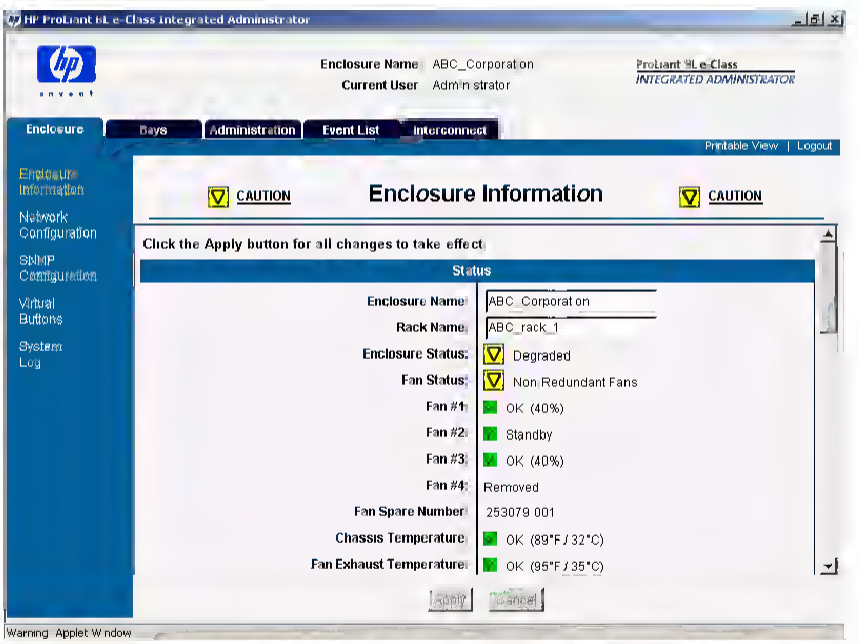


Figure 6-7: Viewing the Web-based user interface of the Integrated Administrator during a fan failure

You can identify the degraded components in the enclosure and their respective part numbers in the following ways:

- Opening the enclosure system log
- Opening the event list

  The event list differs from the system log in the following ways:

  — Any user can view the event list. Only enclosure administrators can access the system log.

  — The messages in the event list are limited to cautions and critical failures. Refer to the enclosure system log for information on fixes.

  — The event list only displays messages received since the user logged into the Integrated Administrator. The system log displays every message generated by the enclosure diagnostics.

- Clicking on the **Caution** or **Critical** icon along the top of the deck panel

  This action opens the event list. By highlighting an item in the event list and clicking **View Event Details**, you can access the area within the Integrated Administrator that provides detailed information about that degraded component.

  IMPORTANT: As soon as you click the **Caution** or **Critical** icon, that icon disappears whether the degraded conditions are corrected or not.

To identify a degraded component using the System Log from the Web-based user interface:

1. Click on the **Enclosure** tab.
2. Click on **System Log** in the left panel.

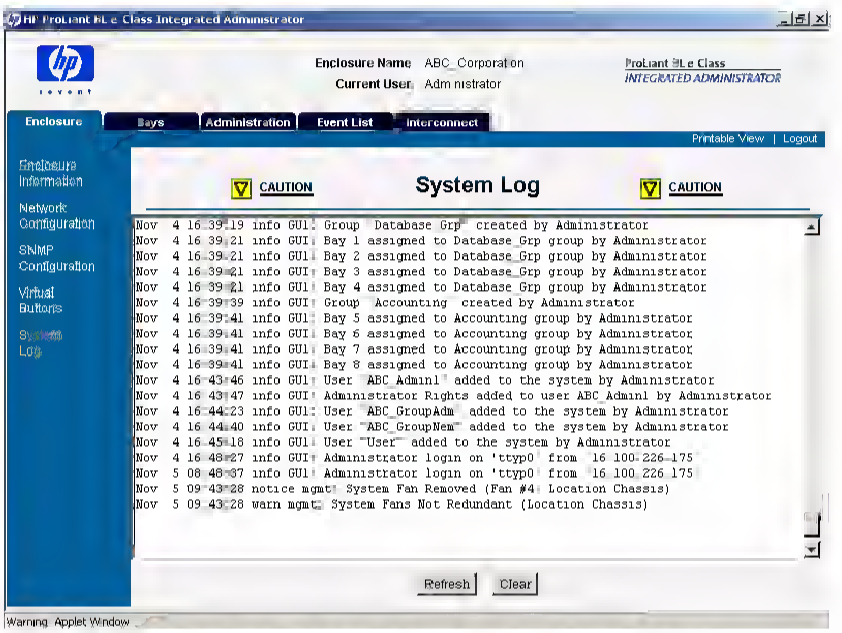

Enclosure Name ABC_Corporation
Current User Administrator
ProLiant BLe Class
INTEGRATED ADMINISTRATOR
Enclosure
Bays
Administration
Event List
Interconnect
Printable View | Logout
Enclosure Information
Network Configuration
SNMP Configuration
Virtual Buttons
System Log
CAUTION
System Log
CAUTION
Nov 4 16:39:19 info GUI: Group "Database_Grp" created by Administrator
Nov 4 16:39:21 info GUI: Bay 1 assigned to Database_Grp group by Administrator
Nov 4 16:39:21 info GUI: Bay 2 assigned to Database_Grp group by Administrator
Nov 4 16:39:21 info GUI: Bay 3 assigned to Database_Grp group by Administrator
Nov 4 16:39:21 info GUI: Bay 4 assigned to Database_Grp group by Administrator
Nov 4 16:39:39 info GUI: Group "Accounting" created by Administrator
Nov 4 16:39:41 info GUI: Bay 5 assigned to Accounting group by Administrator
Nov 4 16:39:41 info GUI: Bay 6 assigned to Accounting group by Administrator
Nov 4 16:39:41 info GUI: Bay 7 assigned to Accounting group by Administrator
Nov 4 16:39:41 info GUI: Bay 8 assigned to Accounting group by Administrator
Nov 4 16:43:46 info GUI: User "ABC_Admin1" added to the system by Administrator
Nov 4 16:43:47 info GUI: Administrator Rights added to user ABC_Admin1 by Administrator
Nov 4 16:44:23 info GUI: User "ABC_GroupAdm" added to the system by Administrator
Nov 4 16:44:40 info GUI: User "ABC_GroupNem" added to the system by Administrator
Nov 4 16:45:18 info GUI: User "User" added to the system by Administrator
Nov 4 16:48:27 info GUI: Administrator login on 'ttyp0' from 16.100.226.175
Nov 5 08:48:37 info GUI: Administrator login on 'ttyp0' from 16.100.226.175
Nov 5 09:43:28 notice mgmt: System Fan Removed (Fan #4, Location Chassis)
Nov 5 09:43:28 warn mgmt: System Fans Not Redundant (Location Chassis)
Refresh
Clear
Warning: Applet Window

Figure 6-8: Viewing the enclosure system log during a fan failure (Fan 1 removed)

3. Go to the appropriate area in the Integrated Administrator for the spare number of tbe degraded component.

To identify a degraded component using the event list from the Web-based user interface:

1. Click the **Event List** tab.

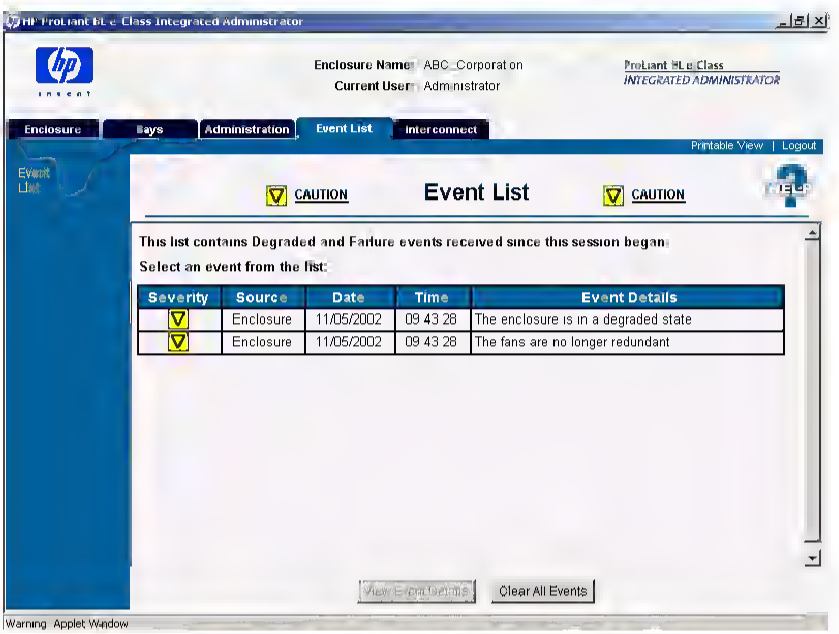


Figure 6-9: Viewing the event list during a fan failure

2. Click the degraded item in the event list.
3. Click **View Event Details** along the bottom of the screen.

   This action opens the page in the Integrated Administrator that displays information about the degraded component.

To identify a degraded component using the **Caution** or **Critical** icons along the top of the deck panel from the Web-based user interface, click an icon. This action opens the event list.

By highlighting an item in the event list and clicking **View Event Details**, you can access the area within the Integrated Administrator that provides detailed information about that degraded component.

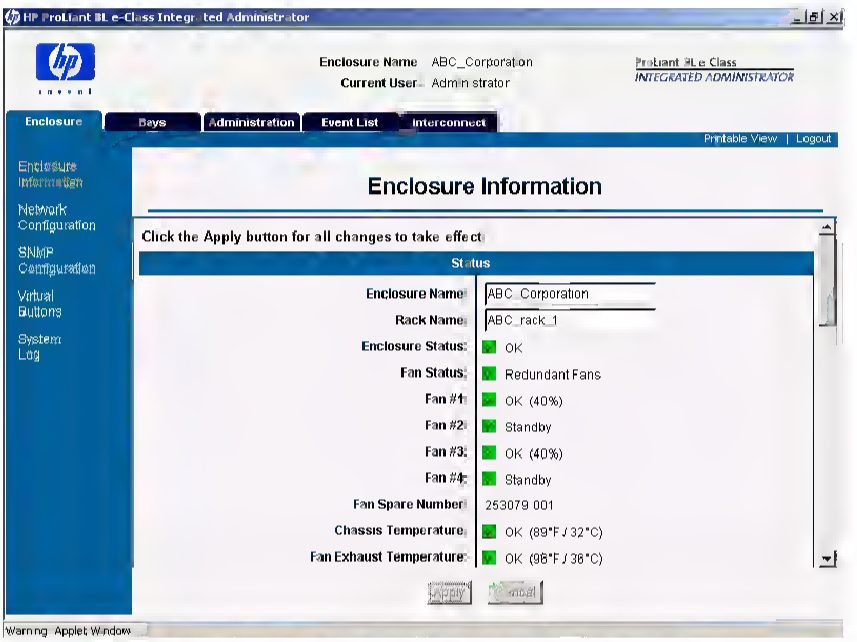


Figure 6-10: Identifying the part number of the fan

To identify a degraded component using the CLI:

1. Enter:

```
SET DISPLAY EVENTS [ON | OFF]
```

IMPORTANT: Choosing the on option for this command ensures that all users are able to see failures as they occur while they are logged into the Integrated Administrator.

2. Enter the appropriate commands:

```
SHOW ENCLOSURE FAN [<fan number> | ALL]
```

IMPORTANT: This command displays the status, redundancy, partner, speed, and part number for one or all fans in the enclosure.

```
SHOW ENCLOSURE INFO
```

IMPORTANT: This command displays the enclosure name, type, part number, serial number, and asset tag number; the Integrated Administrator software and hardware version; the MAC address of the Integrated Administrator, and the interconnect tray type, part number, and serial number.

```
SHOW ENCLOSURE POWERSUPPLY [<power supply number> | ALL]
```

IMPORTANT: This command displays the status, AC input status, capacity, input voltage range #1 (Volts), input voltage range #2 (Volts), input frequency range (Hz), part number, serial number, and hardware revision for one or both power supplies in the enclosure.

```
SHOW ENCLOSURE STATUS
```

IMPORTANT: This command displays the status of enclosure health, Integrated Administrator health, and the Unit Identification LED under the heading "enclosure status," and displays the status and capacity of the power supplies of the enclosure under the heading "power status."

```
SHOW ENCLOSURE TEMP
```

IMPORTANT: This command displays the location, status (OK, warm, degraded, or failed), and temperature (degrees Fahrenheit or Celsius) for all the temperature sensors of the enclosure.

Managing Users

IMPORTANT: Only enclosure administrators may perform these tasks.

IMPORTANT: Restricted default names of group and user accounts (Administrator, switcha, and switchb) are not case-sensitive. Non-default group and user names are case-sensitive.

Modifying a User's Rights to Server Blade Bays

You can only modify a user's rights to server blade bays by modifying their group rights, specifically by choosing one of the following methods:

- Creating a new group for the user with the updated access rights to the server blade bays
- Modifying the rights to server blade bays for a group to which the user has membership

Creating a New Group with the Updated Access Rights

To create a new group with the updated server blade access profile you wish to assign your user, see the "Adding a Group" section in Chapter 5, "Setting Up the System."

Modifying Group Rights to Server Blade Bays

To modify group rights to server blade bays using the Web-based user interface:

1. Click the **Administration** tab.
2. Click **Group List** in the left panel.

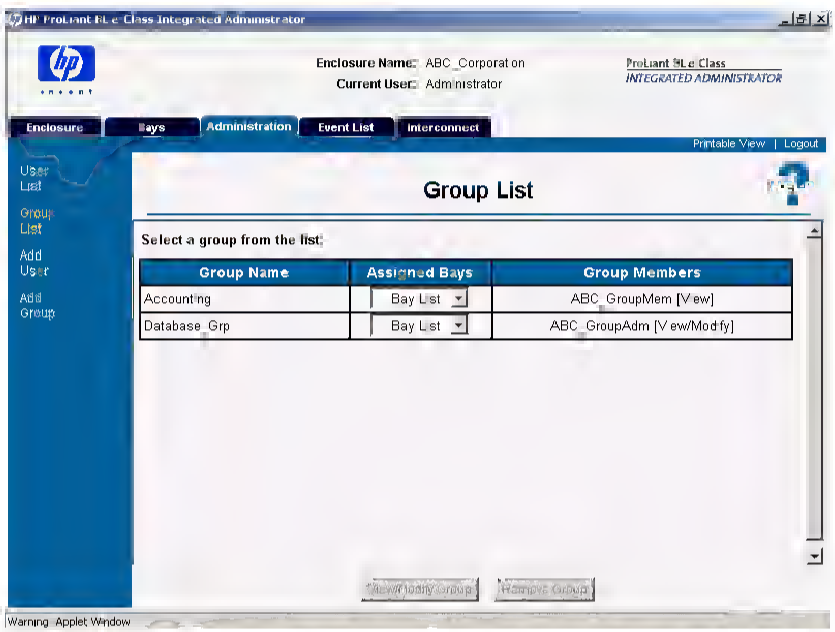


Figure 6-11: Choosing a group from the group list

3. Click on the group whose rights you wish to modify.

4. Click **View/Modify Group**.

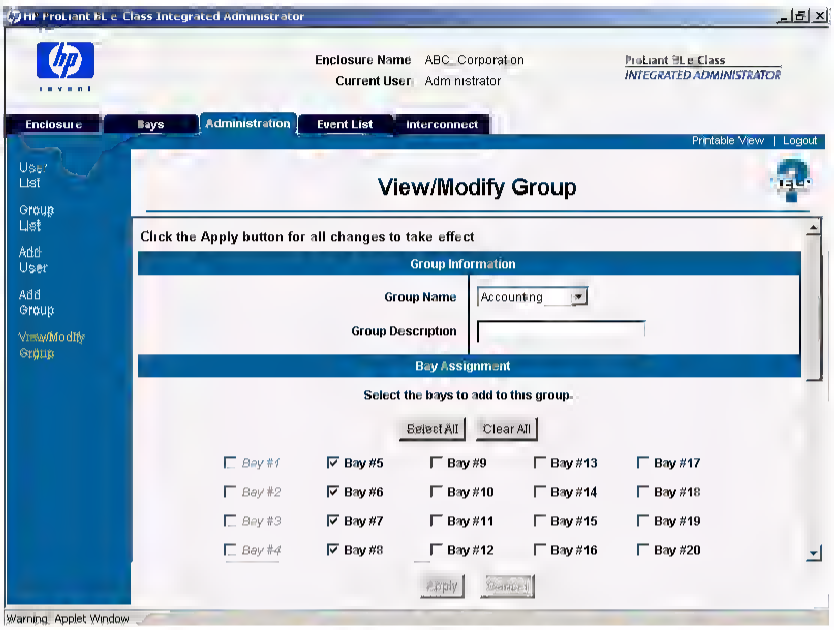


Figure 6-12: Accessing the View/Modify Group screen

5. Select the appropriate checkboxes for the available server blade bays that reflects the updated rights you wish to give the group.

   IMPORTANT: Grayed-out checkboxes are unavailable because they are already assigned to another group.

6. Click **Apply**.

To modify rights to server blade bays for an existing group using the CLI, choose from among the following commands:

IMPORTANT: Only enclosure administrators may execute these commands.

- To expand the number of server blades assigned to a group, enter:

  ```
  ASSIGN BAY [ALL | <bay number> {[ , | - ]<bay number>}]
  <group name>
  ```

  IMPORTANT: If a server blade bay is currently assigned to a group, this command re-assigns the bay from its current group to the new group.

- To remove access rights to server blade bays for any group, enter:

  ```
  UNASSIGN BAY [ALL | <bay number> {[ , | - ] <bay number>}]
  ```

Disabling and Deleting User Accounts

IMPORTANT: Only enclosure administrators may execute this command. Group accounts can be deleted, but cannot be disabled.

To disable a user account using the Web-based user interface:

1. Click the **Administration** tab.
2. Click on **User List** in the left panel.
3. Select the user whose account you wish to disable from the user list.

4. Click **View/Modify User**.

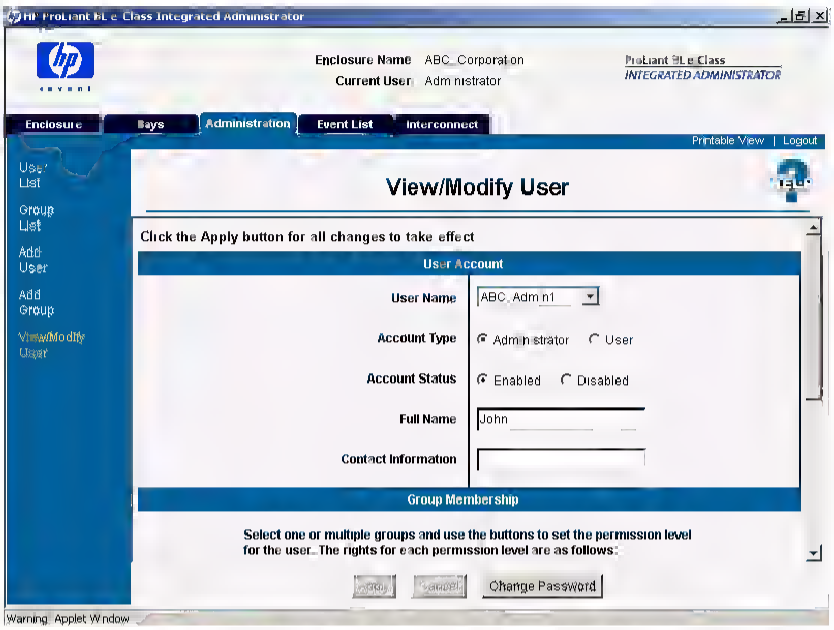


Figure 6-13: Accessing the View/Modify User screen

5. Set the account status to **Disabled**.
6. Click **Apply**.

To disable a user account using the CLI, enter:

```
DISABLE USER <user name>
```

IMPORTANT: When this command is executed, the user is immediately logged out of the system and prevented from logging in until the account is enabled.

Deleting a User's Account

To delete a user account using the Web-based user interface:

1. Click the **Administration** tab.
2. Click **User List** in the left panel.

3. Select the user account you wish to delete from the user list.

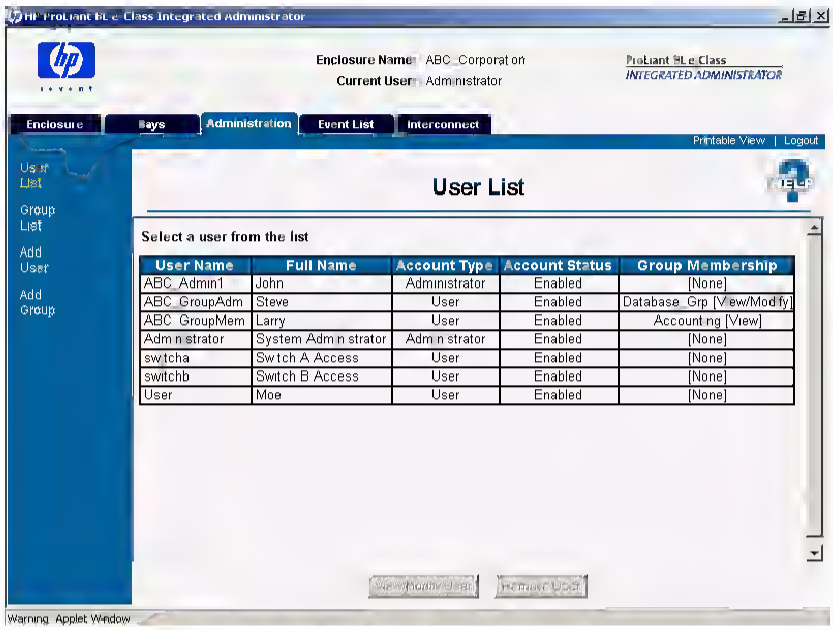

HP ProLiant BL e-Class Integrated Administrator
Enclosure Name: ABC_Corporation
Current User: Administrator
ProLiant BL e-Class
INTEGRATED ADMINISTRATOR
Enclosure
Bays
Administration
Event List
Interconnect
Printable View | Logout
User List
Group List
Add User
Add Group
User List
Select a user from the list
User Name | Full Name | Account Type | Account Status | Group Membership
ABC_Admin1 | John | Administrator | Enabled | [None]
ABC_GroupAdm | Steve | User | Enabled | Database_Grp [View/Modify]
ABC_GroupMem | Larry | User | Enabled | Accounting [View]
Administrator | System Administrator | Administrator | Enabled | [None]
switcha | Switch A Access | User | Enabled | [None]
switchb | Switch B Access | User | Enabled | [None]
User | Moe | User | Enabled | [None]
Warning: Applet Window

Figure 6-14: Accessing the user list

4. Click **Remove User**.

To delete a user account using the CLI, enter:

```
REMOVE USER [ALL | <user name>]
```

IMPORTANT: If ALL is specified, the command deletes all the user accounts except the "Administrator" account. The "Administrator" account cannot be removed.

Deleting Group Accounts

To delete a group account using the Web-based user interface:

1. Click the **Administration** tab.
2. Click **Group List** in the left panel.

3. Select the group from the group list.

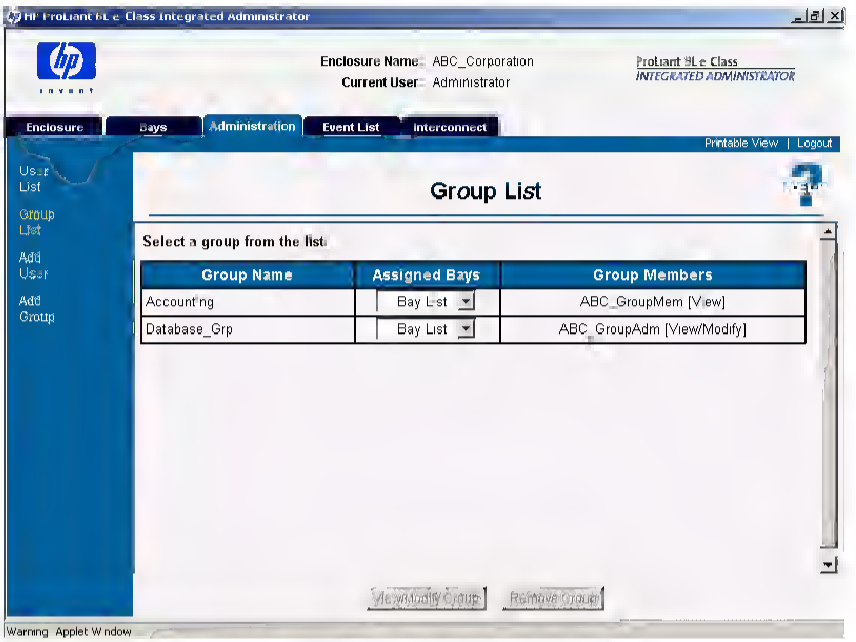


Figure 6-15: Accessing the group list

4. Click **Remove Group**.

To delete a group account using the CLI, enter:

```
REMOVE GROUP [ALL | <group name>]
```

IMPORTANT: If ALL is specified, the command deletes all the group accounts.

7

Performing Advanced Functions

This chapter provides an explanation of the following advanced tasks you can perform using the Integrated Administrator. These procedures are supported by the Web-based user interface and the CLI unless otherwise noted:

- Replicating the configuration of the Integrated Administrator
- Administering security certificates
  - — Creating a security certificate
  - — Downloading a security certificate
- Key-Based SSH Authentication
- Configuring a Server Blade Boot Order
- Powering off the enclosure
- Disabling network protocols to the Integrated Administrator
- Upgrading the firmware of the Integrated Administrator
- Recovering a lost Administrator password
- Launching flash disaster recovery

IMPORTANT: Only enclosure administrators may perform the tasks in this chapter. For more information on who may perform each task, see the "User Permissions" section in Chapter 5, "Setting Up the System."

Replicating the Configuration of the Integrated Administrator

IMPORTANT: The Integrated Administrator does not support this task using the Web-based user interface.

To set up several enclosures with the same configuration, configure one enclosure (such as add all user accounts, add all groups, and assign bays) and then replicate that configuration on the other enclosures.

To replicate the configuration of the Integrated Administrator using the CLI:

1. Login as Administrator on the first enclosure.
2. Enter:

   ```
   UPLOAD CONFIG <url>
   ```

   This command uploads the current runtime configuration to the specified TFTP or FTP server. If your FTP server does not allow anonymous uploading, specify an FTP username and password using the syntax:

   ftp://username:password@ftpserver/filename

3. Edit the uploaded configuration file using a text editor to customize the configuration (such as usernames, passwords, and network settings) for the other enclosures.

   IMPORTANT: Step 4 only applies if the other enclosures have been configured previously.

   NOTE: For security reasons, passwords are never replicated in the configuration file.

4. Restore the factory defaults on each of the other enclosures to clear any previous configuration:

   a. Login as Administrator on an enclosure to which you intend to replicate the configuration.

   b. Enter:

      `SET FACTORY`

      This command sets the Integrated Administrator back to its factory default settings, although the password of the "Administrator" account does not change. The Integrated Administrator is restarted after all the changes are implemented.

   IMPORTANT: Only the Administrator account may execute this command.

5. Download the configuration to each of the other enclosures:

   a. Login as Administrator on an enclosure to which you intend to replicate the configuration.

   b. Enter:

      `DOWNLOAD CONFIG <url>`

      The Integrated Administrator does not check the configuration file for errors, but auto-executes the file in script mode. The file is not allowed to change the password of the "Administrator" account. Supported protocols are http, ftp, and tftp. The URL should be formatted as protocol://host/path/file. If your ftp server does not support anonymous connections, specify a username and password by replacing the host part in the above format with username:password@host.

   IMPORTANT: Step C only applies only if you did not set user account passwords in the configuration file.

   c. Set the password for each user account. For commands, see Table 4-3, "User Account Commands" in Chapter 4, "Command Line Interface."

Administering Security Certificates

IMPORTANT: The Integrated Administrator does not support these tasks using the Web-based user interface.

Creating a Certificate Request

To create a security certificate using the CLI, enter:

```
GENERATE CERTIFICATE REQUEST
```

This command generates a PKCS#10 certificate request. This certificate request can be sent to your certification authority (CA) to obtain a PKCS#7 certificate file to use below.

To create a self-signed security certificate using the CLI, enter:

```
GENERATE CERTIFICATE SELFSIGNED
```

This command generates a self-signed PKCS#7 certificate to replace the existing SSL certificate. This certificate is signed with the current name of the enclosure and will be valid for 10 years. Users who do not have a certificate authority (CA) may use this certificate as a replacement.

Downloading a Security Certificate

To download a security certificate using the CLI, enter:

```
DOWNLOAD CERTIFICATE <url>
```

This command downloads a CA supplied PKCS#7 file to replace the current security certificate on the system.

Supported protocols are http, ftp, and tftp. The URL should be formatted:

protocol://host/path/file

If your ftp server does not support anonymous connections, you can specify a username and password by replacing the host part in the previous format:

username:password@host

Key-Based SSH Authentication

Users may install their own public SSH keys for password-less logins to the Integrated Administrators. Only enclosure administrators can use key-based authentication. The CLI features four commands to install and manage the authorized SSH keys.

To view any current installed authorized SSH keys, enter:

```
SHOW SSHKEY
```

This command will show any keys currently installed on the Integrated Administrator that are authorized to log in using an enclosure administrator account.

To view the fingerprint of the Integrated Administrator host key, enter:

```
SHOW SSHFINGERPRINT
```

This command will show the fingerprint of the host key for the Integrated Administrators. Users may compare this fingerprint with the fingerprint displayed by their SSH client when connecting to the Integrated Administrators to guarantee the authenticity of tbe Integrated Administrator connection. Users who need guaranteed authenticity will want to use the Integrated Administrator serial console to obtain the SSH fingerprint for the first time.

To clear any currently installed authorized SSH keys, enter:

```
CLEAR SSHKEY
```

This command will clear any authorized keys currently installed on the Integrated Administrator that are authorized to log in. After this command has been issued, all users have to enter a valid password in order to log in.

To download and install one or more SSH keys, enter:

```
DOWNLOAD SSHKEY <URL>
```

This command will download and install a file containing one or more SSH keys which are authorized to log into the Integrated Administrator. The new file will replace any existing keys.

Supported protocols are http, ftp and tftp. The URL should be formatted like the following:

protocol://host/path/file

If your ftp server does not support anonymous logins, you can specify a username and password by replacing the bost part (in previous format) with:

username:password@host

The Integrated Administrator supports multiple SSH keys in one downloaded file. Max file size for SSH keys is 16K.

Key-based SSH logins has an advantage for use with scripting as well. Remote commands can be sent to any Integrated Administrator after installing the appropriate authorized key without having to enter a password between each command. Using the OpenSSH package, the user can send commands using the following syntax:

```
ssh user@host command
```

Commands can be grouped together to perform a series of actions. To view the health status of the enclosure and all blades with a single command, enter:

```
ssh user@host "SHOW ENCLOSURE STATUS; SHOW STATUS BAY ALL"
```

By having an authorized key file installed on the Integrated Administrator, the user can combine these without having to enter a password between each command sent to the Integrated Administrator.

Configuring Server Blade Boot Order

Enclosure and group administrators may change the boot order, sometimes referred to as Initial Program Load (IPL), of their server blades by using the CLI of the Integrated Administrator. The change can be made permanently or only for the next reboot. Several commands are available in the CLI to control the blades in this manner. This feature requires version 1.20 or higher of the Integrated Administrator firmware and a blade ROM dated 06/15/02 or newer to be controlled in this manner.

To set a server blade boot order, enter:

```
SET BAY BOOT FIRST [HDD | PXE] [ALL | <bay number> {[,|-]
<bay number>}]
```

During the next reboot, this will set the specified server blade boot order to use the given boot device first. This has the same effect as changing the Standard Boot Order (IPL) setting in the RBSU on the server blade.

To set a server blade boot order for the next boot only, enter:

```
SET BAY BOOT ONCE [HDD | PXE | RBSU] [ALL | <bay number>
{[,|-] <bay number>}]
```

This will force the specified server blade to boot to the specified media on the next boot only. The RBSU setting will make the server(s) boot into the RBSU which can be viewed with the Remote Console functionality. The HDD setting forces the server blade to boot from the hard drive first, and the PXE setting forces it to boot from the integrated NIC first.

To reset blade boot order settings which have not yet taken effect, enter:

```
CLEAR BAY BOOT [FIRST | ONCE] [ALL | <bay number> {[,|-]
<bay number>}]
```

This will clear changes to the specified server boot order that were made with the `SET BAY BOOT` command. It only affects pending changes so if the server blade has been rebooted since the `SET BAY BOOT` command, this command will have no effect.

The POWERON BAY and REBOOT BAY commands have been extended to allow an argument which sets server blade boot order for that boot only. These settings are the same as the SET BAY BOOT ONCE command.

To determine if any boot order changes are pending for a specific blade, use the SHOW BAY INFO command. The "Pending Boot Order:" status line will show any pending changes to the boot order, either one-time or permanent.

Powering Off the Enclosure

CAUTION: Powering off the enclosure removes all power from the server blades and ends all open sessions. After powering off the enclosure, you can only power on the enclosure if you have physical access to the enclosure.

To power off the enclosure using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **Virtual Buttons** in the left panel.

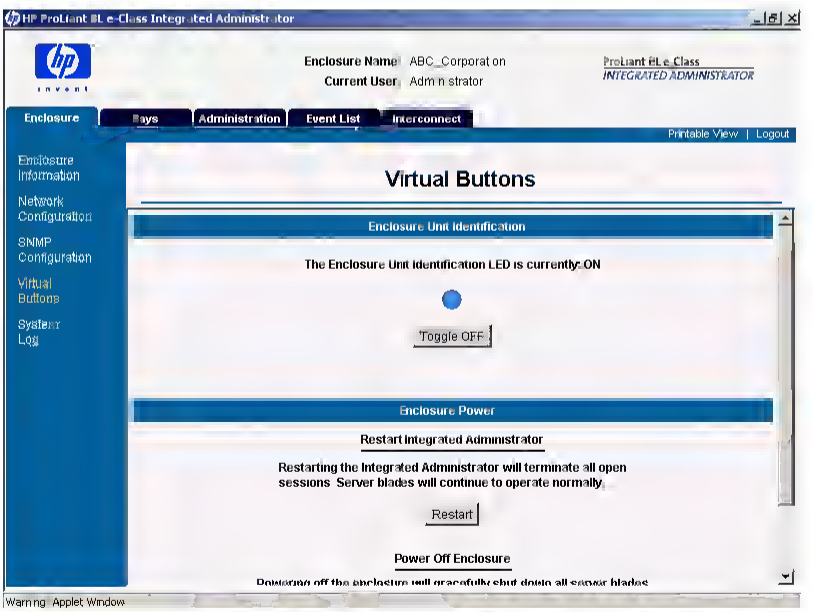


Figure 7-1: Accessing Virtual Buttons

3. Click **Power Off**.
4. Click **Apply**.

To power off the enclosure using the CLI, enter:

```
POWEROFF ENCLOSURE
```

This command attempts to perform a graceful shutdown of the enclosure by powering off each server blade and then powering off the enclosure. After 5 minutes, the command powers down all components of the system immediately if they are not already powered off.

CAUTION: Without the server blade health driver or an ACPI-compliant operating system, the Integrated Administrator cannot gracefully shutdown a server blade. This condition may result in the permanent loss of critical data.

Disabling Network Protocols

To modify the supported communications protocols of the enclosure using the Web-based user interface:

1. Click the **Enclosure** tab.
2. Click **Network Configuration** in the left panel.

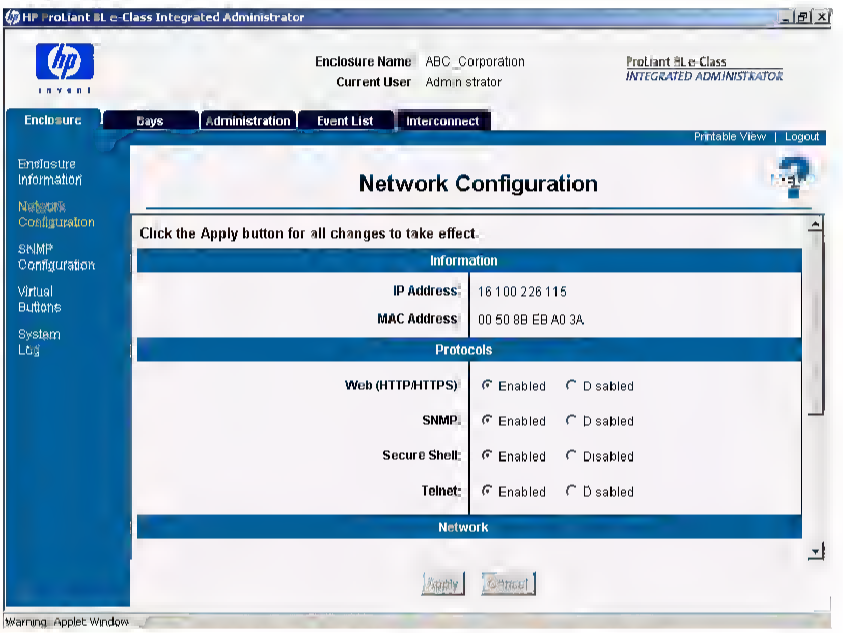


Figure 7-2: Accessing the Network Configuration screen

3. Select the appropriate radio buttons in the **Protocols** area.
4. Click **Apply**.

To modify the supported communications protocols of the enclosure using the CLI, choose from among the following commands:

- To disable http/https communication, enter:

```
DISABLE WEB
```

- To disable automatic time updates, enter:

```
DISABLE NTP
```

IMPORTANT: Disabling http/https causes the users to lose access to the Web-based user interface.

- To disable SNMP communication, enter:

```
DISABLE SNMP
```

- To disable Secure Shell communication, enter:

```
DISABLE SECURESH
```

IMPORTANT: Disabling Secure Shell causes the users to lose access to the Web-based user interface.

- To disable telnet communication, enter:

```
DISABLE TELNET
```

Upgrading the Integrated Administrator Firmware

The firmware associated with the Integrated Administrator can be upgraded remotely using the CLI using the management (10/100 Ethernet) connector located on the rear panel of the enclosure. See Table 4-5, "Enclosure Management Commands," for detailed information on the following command used to perform this function:

```
UPDATE IMAGE <url>
```

IMPORTANT: <URL> can be any of the following:

- http://*host/path*
- tftp://*host/path*
- ftp://*username:password@host/path*
- ftp://*host/path*

where *host* is a fully qualified domain name or an IP address and *path* is the pathname of the flash image to download.

Refer to the documentation associated with the firmware upgrade for detailed information.

Recovering a Lost Administrator Password

To recover a lost Administrator password:

1. Be sure the local client device is properly configured for local access to the Integrated Administrator. See the "Requirements for Local Client Devices" section in Chapter 2, "Getting Started."
2. Connect a local client device to the Integrated Administrator (serial) console connector using the null-modem serial cable (provided with the enclosure).

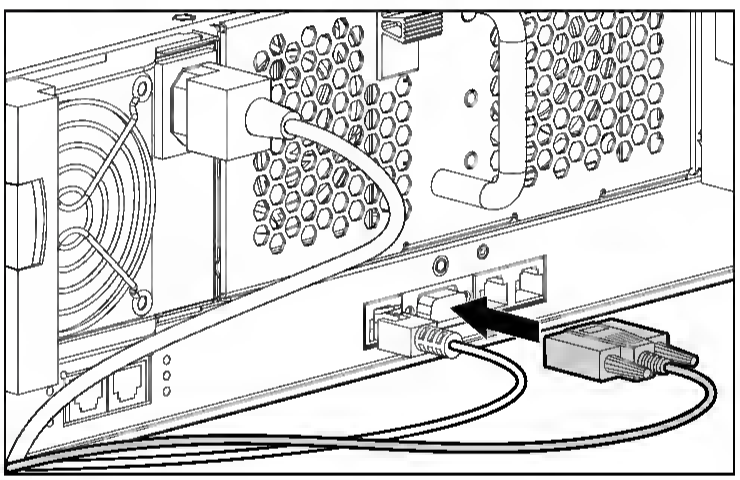


Figure 7-3: Installing a local client device to the Integrated Administrator (serial) console connector

3. Open a terminal emulation application.
4. Press and hold the enclosure Unit Identification button (1) and press the Integrated Administrator Reset button (2) simultaneously on the rear panel of the server to place the enclosure in Lost Password/Flash Disaster Recovery mode.

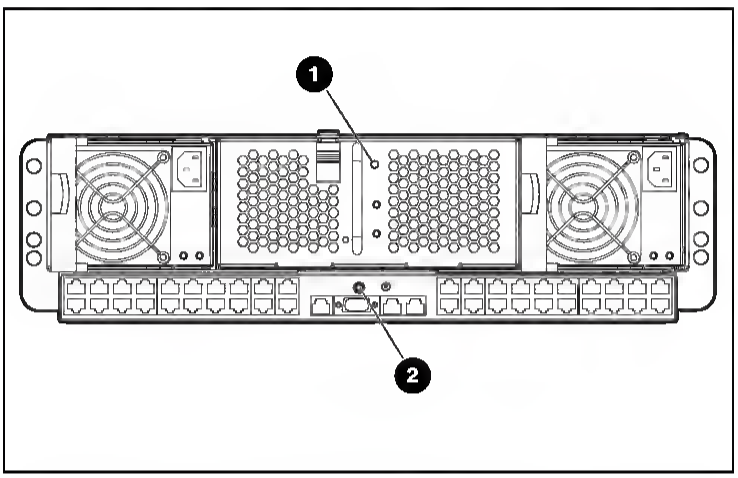


Figure 7-4: Enclosure Unit Identification button and the Integrated Administrator Reset button

5. When the serial console prompt appears, press the **L** key.

   This command boots the system in Lost Password mode, which resets the Administrator password to the factory default and displays it on the console.

Launching Flash Disaster Recovery

Flash Recovery mode requires the following items:

- DHCP server
- TFTP server
- A connection to the Integrated Administrator serial console
- Integrated Administrator ROM image file on the TFTP server

IMPORTANT: The filename of the ROM image of the Integrated Administrator can be any valid ASCII filename. The ROM image of the Integrated Administrator can be any valid image that supports the "update image" facility in the operating system.

The Integrated Administrator will automatically enter Flash Recovery mode when a corrupted image is detected. Flash Recovery mode can also be manually initiated.

IMPORTANT: No timeout exists for obtaining a DHCP address.

The Flash Recovery process should only be initiated when the Integrated Administrator fails to boot properly because an operating system image is corrupted by some unforeseen problem, such as a power/catastrophic failure during the standard "update image" flash procedure.

Flash Recovery mode makes every attempt to successfully flash the operating system image of the Integrated Administrator. The only way to leave Flash Recovery mode without successfully updating the image is to reset the Integrated Administrator.

You can manually place the Integrated Administrator in Flash Recovery mode:

1. Connect a local client device to the Integrated Administrator (serial) console connector using the null-modem serial cable (provided with the enclosure). See the "Requirements for Local Client Devices" section in Chapter 2, "Getting Started."

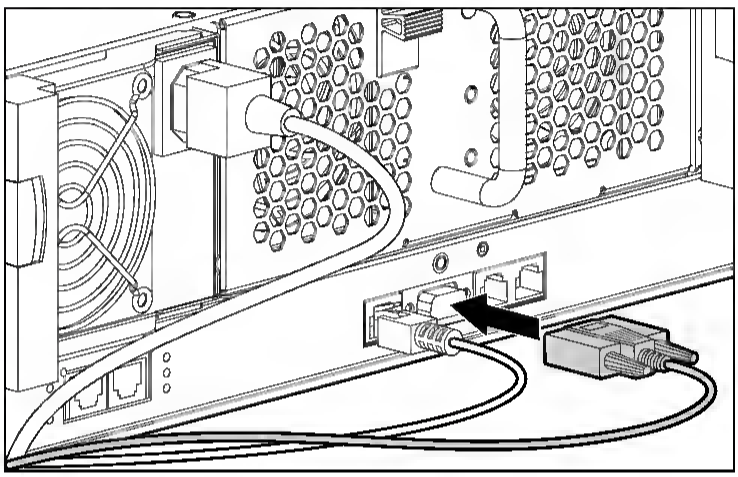


Figure 7-5: Installing a local client device to the Integrated Administrator (serial) console connector

2. Press and hold the enclosure Unit Identification button (1) and press the Integrated Administrator Reset button (2) simultaneously on the rear panel of the server to place the enclosure in Lost Password/Flash Disaster Recovery mode.

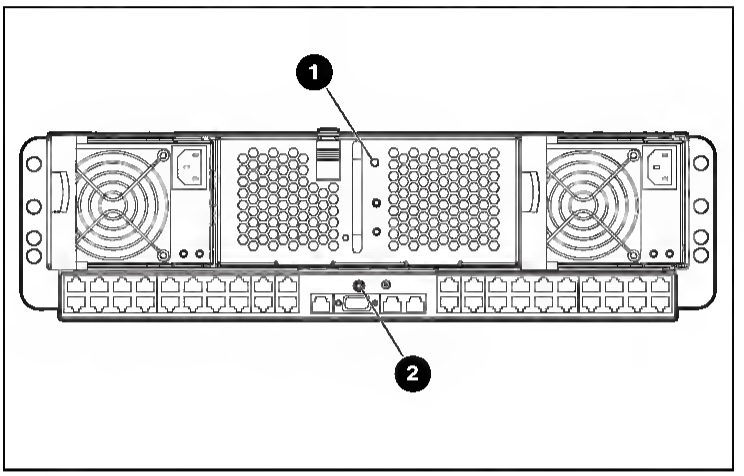


Figure 7-6: Enclosure Unit Identification button and the Integrated Administrator Reset button

3. When the serial console prompt appears, press the **F** key.

   IMPORTANT: This command is case-insensitive.

   Pressing the **L** key launches Lost Password recovery mode. Pressing any other key exits Lost Password/Flash Disaster Recovery mode and reboots the system.

   This command boots the system in Flash Disaster Recovery mode, prints a message, and resets the enclosure.

   Upon entering Flash Disaster Recovery mode, the Integrated Administrator attempts to acquire a DHCP address. If successful, the Integrated Administrator prompts the user for:

   — IP address of the TFTP server

   — Filename of the ROM on the TFTP server

   The Integrated Administrator then downloads and verifies the ROM and updates the flash memory.

   IMPORTANT: No timeout exists for obtaining a DHCP address.

   IMPORTANT: If the ROM does not download properly or if the verification step fails, Flash Disaster Recovery mode restarts with another attempt to acquire a DHCP address.

   The Integrated Administrator reboots.

A

Command Line Conventions

The following sections provide commands for the CLI using the convention described in Table A-1:

Table A-1: Command Line Conventions

Symbol	Description
<lower case>	Denotes input to be keyed in
UPPER CASE	Denotes input to be keyed in as shown
[ ]	Denotes choices to be made where a choice is mandatory
{ }	Denotes choices to be made where a choice is optional
|	Separates input options
" "	Used to enclose arguments that contain spaces

For example, the following command requires the user to input whether the Integrated Administrator is operating in a "DHCP" or "Static" network environment:

```
SET IPCONFIG [DHCP {DYNAMICDNS} | STATIC <IP address>
<netmask>]
```

Specifying "Dynamic DNS" is optional for executing this command for the DHCP environment, but specifying the IP address and netmask are required for executing this command for the static environment.

B

Error Messages

The messages provided in this appendix are divided into the following categories:

- Warning messages
- Error messages

Warning Messages

This section provides a comprehensive list of warning messages specific to the major components of the Integrated Administrator. These warning messages advise you that you have implemented a configuration change or prompt you to confirm whether you wish to proceed with your requested action.

Enclosure Warning Messages

Table B-1: Enclosure Warning Messages

Warning Message	Cause
Are you sure you want to disable the Web protocol? Disabling this protocol will prevent access to the Web-based user interface until a terminal session re-enables the Web protocol.	Attempting to disable the Web (HTTP / HTTPS) protocol
Are you sure you want to disable the Secure Shell protocol? Disabling this protocol will prevent access to the Web-based user interface and Secure Shell terminal interface until a terminal session re-enables the Secure Shell protocol.	Attempting to disable the Secure Shell protocol
The SNMP protocol is currently disabled. The new settings will not take effect until this protocol is enabled on the Network Configuration screen.	Changing an SNMP value with the SNMP protocol disabled
The Read Community field is empty. The Read Community will be set to "public". The SNMP protocol may be disabled on the Network Configuration screen.	Attempting to set a blank Read Community string
Are you sure that you want to power off the enclosure?	Attempting to power off the enclosure
Are you sure that you want to restart the Integrated Administrator? This process will take several minutes.	Attempting to restart the Integrated Administrator
Are you sure that you want to clear the system log?	Attempting to clear the system log
Enabling IP Security may disconnect this session. Are you sure you still want to perform this action?	Attempting to enable IP Security

Server Blade Bay Warning Messages

Table B-2: Server Blade Bay Warning Messages

Warning Message	Cause
This server blade has been removed from the enclosure.	The server blade that is being viewed has been removed from the enclosure.
This server blade has been powered off. All open sessions will be closed.	The current server blade has been powered off.
Are you sure that you want to power off the server blade immediately? This process may result in the loss of any unsaved data on the blade.	Attempting to immediately power off a server blade.

Administration Warning Messages

Table B-3: Administration Warning Messages

Warning Message	Cause
Are you sure you want to permanently remove <user name>? All data for this account will be removed from the system.	Attempting to delete a user
Are you sure you want to permanently remove <group name>? All bays in this group will be unassigned and the data for this group will be permanently removed from the system.	Attempting to delete a group

Error Messages

This section provides a comprehensive list of error messages specific to the major components of the Integrated Administrator. These error messages advise you that an error has occurred during the normal operation of the Integrated Administrator.

Enclosure Error Messages

Table B-4: Enclosure Error Messages

Error Message	Cause	Valid Input
The maximum number (8) of trap destinations has been reached.	Attempting to add a 9th trap destination	N/A
The trap destination of ###.###.###.### is already on the list. Enter a new value.	Attempting to add a duplicate trap destination	N/A
An error occurred while clearing the system log. Please try again.	Attempting to clear the system log	N/A

Server Blade Bay Error Messages

Table B-5: Server Blade Bay Error Messages

Error Message	Cause	Valid Input
You no longer have permissions to view this bay.	User permission change	N/A

Administration Error Messages

Table B-6: Administration Error Messages

Error Message	Cause	Valid Input
The user name field is empty. Please enter a user name.	Attempting to create a user with a blank user name	1-13 characters including alphanumeric, dash, and underscore characters. The user name must begin with a letter.
This user name already exists. Please select a different user name.	Attempting to create a user without a unique user name	1-13 characters including alphanumeric, dash, and underscore characters. The user name must begin with a letter.
The Password fields are empty. Please enter a value in each password field.	Attempting to create a user with a blank password	3-8 characters including all printable characters
The Password field is empty. Please enter a password.	Attempting to create a user with a blank **Password** field	3-8 characters including all printable characters
The Confirm Password field is empty. Please enter a password.	Attempting to create a user with a blank **Confirm Password** field	3-8 characters including all printable characters
The password must be at least 3 characters in length. Please enter a new password.	Attempting to create a user with a password that is less than 3 characters long	3-8 characters including all printable characters
The passwords do not match. Please try again.	Different strings in the **Password** and **Confirm Password** fields	3-8 characters including all printable characters
The maximum number (25) of users exists on the system.	Attempting to create a 26th user	N/A

continued

Table B-6: Administration Error Messages *continued*

Error Message	Cause	Valid Input
The group name is blank. Please enter a valid name.	Attempting to create a group with a blank group name	1-13 characters including alphanumeric, dash, and underscore characters The group name must begin with a letter.
The maximum number (20) of groups exists on the system.	Attempting to create a 21st group	N/A
The Password fields are empty. Please enter a value in each password field.	Attempting to create a user with a blank password	3-8 characters including all printable characters
The Password field is empty. Please enter a password.	Attempting to create a user with a blank **Password** field	3-8 characters including all printable characters
The Confirm Password field is empty. Please enter a password.	Attempting to create a user with a blank **Confirm Password** field	3-8 characters including all printable characters
The password must be at least 3 characters in length. Please enter a new password.	Attempting to create a user with a password that is less that 3 characters long	3-8 characters including all printable characters
The passwords do not match. Please try again.	Different strings in the **Password** and **Confirm Password** fields	3-8 characters including all printable characters
NTP Poll-Interval has to be between 60 and 9999 seconds.	Attempting to set an NTP poll interval that is not between 60 and 9999 seconds.	60-9999
Invalid NTP address supplied. IP address should be in ###.###.###.### format where ### is between 0 and 255.	Attempting to enter an IP address that is not in the correct format.	###.###.###.### where ### is between 0 and 255
###.###.###.### is not a valid NTP server.	Attempting to set an NTP server address, but the address entered is not an NTP server.	N/A

continued

Table B-6: Administration Error Messages *continued*

Error Message	Cause	Valid Input
Please set at least the Primary NTP server before enabling NTP.	Attempting to enable the NTP server before enabling the primary NTP server set.	N/A
<IP address> is already set as secondary NTP server.	Attempting to set the primary NTP server to *<IP address>* when the *<IP address>* is already set as secondary.	N/A
<IP address> is already set as primary NTP server.	Attempting to set the primary NTP server to *<IP address>* when the *<IP address>* is already set as secondary.	N/A
Primary NTP server is already cleared.	Attempting to clear the primary NTP server that has previously been cleared or never set.	N/A
The secondary NTP server is already cleared.	Attempting to clear the secondary NTP server that has previously been cleared or never set.	N/A
Please set the primary NTP server first.	Attempting to set the secondary NTP server without first setting the primary NTP server.	N/A
Invalid IP address supplied. IP address should be in ###.###.###.### or ###.###.###.###/## format where ### is between 0 and 255 and ## is between 0 and 32.	Attempting to set an IP address that is not in the correct format.	###.###.###.### where ### is between 0 and 255 and ## is between 0 and 32.
Invalid e-mail address supplied. Address should be in user@domain.tld format.	Attempting to enter an e-mail address that is not in the correct format.	E-mail addresses formatted "user@domain.tld" and containing a maximum of 64 characters.
E-mail address is too long. Length must be less than 65 characters.	Attempting to enter an e-mail address containing more than 64 characters.	E-mail addresses formatted "user@domain.tld" and containing a maximum of 64 characters.

C

Troubleshooting

This appendix provides troubleshooting information for the Integrated Administrator that ships as part of the ProLiant BL e-Class system. Use it to find details about solving performance problems that may arise when viewing or managing enclosure, server blade, or user information using the Integrated Administrator.

For information on troubleshooting hardware for the ProLiant BL e-Class system, refer to the *HP ProLiant BL e-Class System Setup and Installation Guide*.

For information on LEDs and switches specific to the server blades and enclosure, refer to the *HP ProLiant BL e-Class System Setup and Installation Guide*.

For information about general troubleshooting techniques, diagnostic tools, error messages, and preventative maintenance, refer to the *HP Servers Troubleshooting Guide*, also included in the user documentation.

Table C-1: Integrated Administrator Troubleshooting

Problems	Possible Solution
My Web browser flickers when I view the Integrated Administrator applet.	Be sure the client browser has at least 16-bit color depth.
My Web browser is not supported by the Integrated Administrator.	Be sure to use a supported Web browser. For the most up-to-date information on supported Web browsers, please view the customer advisories located at www.compaq.com/support/servers
I am having general browser problems.	For the most recent tips regarding the Integrated Administrator, refer to the customer advisories on the following website: www.compaq.com/support
My Web browser seems unstable when I access the Integrated Administrator.	Your Java Virtual Machine (JVM) must be build 3802 or newer. Netscape users are advised to use Netscape 6.2 or later to include this JVM and Internet Explorer users can download the latest JVM from the Microsoft website: www.microsoft.com/java/ This update is mandatory for Windows 95 and Windows 98 users and is available in Service Pack 2 for Windows 2000 users. For the most up-to-date information on supported Web browsers, please view the customer advisories located at www.compaq.com/support/servers
The Integrated Administrator does not show the most up-to-date blade information. The server blade information is unknown.	The server blade configuration information is exchanged with the Integrated Administrator during the server Power-On Self Test (POST). If the Integrated Administrator is restarted after the server blades have booted, the Integrated Administrator does not display the server blade configuration information until the server blades are rebooted. Also, the server blade BIOS obtains part of the information of the server blade from the health driver; so after installing the health driver, you may need to cycle the server blade power to enable the Integrated Administrator sees new information.

continued

Table C-1: Integrated Administrator Troubleshooting *continued*

Problems	Possible Solution
I just got logged out of the GUI. Why? What should I do?	Your rights may have changed. If so, log in again to use your new rights. If the problem continues, contact the enclosure administrator.
When I ran "upload config," garbage printed to the screen and then a statement printed saying the command completed successfully. Did an error occur?	No error occurred in this command. Everything ran as expected.
My fans periodically increase speed and then return to their normal speed.	Fans perform a self-test for 60 seconds every 24 hours.
Although my username and my password are valid, I am unable to log into the Integrated Administrator.	The Integrated Administrator supports up to 46 concurrent sessions. Be sure the number of sessions has not reached this threshold and check with an enclosure administrator to be sure your account is not disabled.
The Event List does not report event repairs.	The Event list only displays negative events that happen during the user's login session. Although repairs are not listed here, the user may highlight the event and click on **View/Modify** to see the present event status. The user can also view the System Log of the enclosure.

D

Event Details

The Integrated Administrator provides real-time event notifications for an enclosure according to two categories: caution and critical. When an event occurs, the Integrated Administrator notifies the user by generating an icon that the user can click to view more details:

Table D-1: Event Notification Icons

Icon	Description
	Caution—An event that does not prevent the enclosure from operating, maintaining power, or serving its user community When a Caution event occurs, a reasonable guarantee that operability can persist no longer exists.
	Critical—An event that prevents the continued operation of the enclosure When a Critical event occurs, the inoperability of the enclosure is imminent.

The following table provides a comprehensive list of event messages provided by the Integrated Administrator in a format that reflects the display of the Integrated Administrator:

Table D-2: Event Details

Severity	Source	Date	Time	Event Details
	Enclosure	<date>	<time>	The enclosure has experienced a failure.
	Enclosure	<date>	<time>	Fan # has experienced a failure.
	Enclosure	<date>	<time>	Power supply # has experienced a failure.
	Enclosure	<date>	<time>	The enclosure temperature has exceeded the critical threshold.
	Blade in Bay #	<date>	<time>	Blade # has experienced a failure.
	Blade in Bay #	<date>	<time>	The temperature on blade # has exceeded the critical threshold.
	Enclosure	<date>	<time>	The enclosure is in a degraded state.
	Enclosure	<date>	<time>	Fan # is in a degraded state.
	Enclosure	<date>	<time>	The redundancy of the power supplies is in an unknown state.
	Enclosure	<date>	<time>	The power supplies are no longer redundant.
	Enclosure	<date>	<time>	Power supply # is in a degraded state.
	Enclosure	<date>	<time>	The enclosure temperature has exceeded the caution threshold.
	Blade in Bay #	<date>	<time>	Blade # is in a degraded state.
	Blade in Bay #	<date>	<time>	The temperature on blade # has exceeded the caution threshold.

E

Factory Default Settings

This appendix provides the factory default settings for the following components of the ProLiant BL e-Class Integrated Administrator:

- Enclosure
- Users
- Groups
- Network
- Protocol

Enclosure

Table E-1 provides the default values in the Integrated Administrator for fields related to the server blade enclosure.

Table E-1: Default Enclosure Values for the Integrated Administrator

Field	Default Value
Name	IA-*XXXXXXXXXXXX* where *XXXXXXXXXXXX* is the MAC Address of the Integrated Administrator
Rack Name	UnnamedRack
Asset Tag	Blank
Time Zone	CST6CDT

Users

The Integrated Administrator provides the following default users:

- Administrator
- switcha
- switchb

NOTE: The "switcha" and "switchb" accounts are used when accessing the optionally installed interconnect switch console.

Groups

No default groups are in the Integrated Administrator.

Network

The Integrated Administrator ships with the following default values assigned:

Table E-2: Integrated Administrator's Default Network Values

Field	Default Value
DHCP	Enabled
Dynamic DNS	Enabled

Protocol

Table E-3 provides the default values in the Integrated Administrator for fields related to network interface protocols.

Table E-3: Default Protocol Values of Integrated Administrator

Field	Default Value
HTTP	On
SSH	On
TELNET	On
SNMP	On
SNMP location	Blank
SNMP contact	Blank
READ community	Public
WRITE community	Blank
NTP	Disabled

continued

Table E-3: Default Protocol Values of Integrated Administrator *continued*

Field	Default Value
IP Security	Disabled
AlertMail	Disabled

F

Time Zone Settings

This appendix provides a comprehensive list of time zones supported by the ProLiant BL e-Class Integrated Administrator. These time zones are organized into the following categories:

- Universal
- Africa
- Asia
- Europe
- Oceania
- Polar
- The Americas

Universal

Table F-1 provides the Universal time zone settings supported by the Integrated Administrator.

CAUTION: For the Integrated Administrator to recognize GMT time zones, the "Etc:" string must precede them.

Table F-1: Universal Time Zone Settings Supported by the Integrated Administrator

CET	Etc:GMT+9	Etc:GMT-12
CST6CDT	Etc:GMT+10	Etc:GMT-13
EET	Etc:GMT+11	Etc:GMT-14
EST	Etc:GMT+12	Greenwich
EST5EDT	Etc:GMT-0	HST
Etc:GMT	Etc:GMT-1	MET
Etc:GMT0	Etc:GMT-2	MST
Etc:GMT+0	Etc:GMT-3	MST7MDT
Etc:GMT+1	Etc:GMT-4	Navajo
Etc:GMT+2	Etc:GMT-5	PST8PDT
Etc:GMT+3	Etc:GMT-6	UCT
Etc:GMT+4	Etc:GMT-7	Universal
Etc:GMT+5	Etc:GMT-8	UTC
Etc:GMT+6	Etc:GMT-9	WET
Etc:GMT+7	Etc:GMT-10	W-SU
Etc:GMT+8	Etc:GMT-11	Zulu

Africa

Table F-2 provides the African time zone settings supported by the Integrated Administrator.

Table F-2: African Time Zone Settings Supported by the Integrated Administrator

Africa:Abidjan	Africa:Djibouti	Africa:Maputo
Africa:Accra	Africa:Douala	Africa:Maseru
Africa:Addis_Ababa	Africa:El_Aaiun	Africa:Mbabane
Africa:Algiers	Africa:Freetown	Africa:Mogadishu
Africa:Asmera	Africa:Gaborone	Africa:Monrovia
Africa:Bamako	Africa:Harare	Africa:Nairobi
Africa:Bangui	Africa:Johannesburg	Africa:Ndjamena
Africa:Banjul	Africa:Kampala	Africa:Niamey
Africa:Bissau	Africa:Khartoum	Africa:Nouakchott
Africa:Blantyre	Africa:Kigali	Africa:Ouagadougou
Africa:Brazzaville	Africa:Kinshasa	Africa:Porto-Novo
Africa:Bujumbura	Africa:Lagos	Africa:Sao_Tome
Africa:Cairo	Africa:Libreville	Africa:Timbuktu
Africa:Casablanca	Africa:Lome	Africa:Tripoli
Africa:Ceuta	Africa:Luanda	Africa:Tunis
Africa:Conakry	Africa:Lubumbashi	Africa:Windhoek
Africa:Dakar	Africa:Lusaka	Egypt
Africa:Dar_es_Salaam	Africa:Malabo	Libya

Asia

Table F-3 provides the Asian time zone settings supported by the Integrated Administrator.

Table F-3: Asian Time Zone Settings Supported by the Integrated Administrator

Asia:Aden	Asia:Dubai	Asia:Manila
Asia:Almaty	Asia:Dushanbe	Asia:Muscat
Asia:Amman	Asia:Gaza	Asia:Nicosia
Asia:Anadyr	Asia:Harbin	Asia:Novosibirsk
Asia:Aqtau	Asia:Hong_Kong	Asia:Omsk
Asia:Aqtobe	Asia:Hovd	Asia:Phnom_Penh
Asia:Ashgabat	Asia:Irkutsk	Asia:Pyongyang
Asia:Ashkhabad	Asia:Istanbul	Asia:Qatar
Asia:Baghdad	Asia:Jakarta	Asia:Rangoon
Asia:Bahrain	Asia:Jayapura	Asia:Riyadh
Asia:Baku	Asia:Jerusalem	Asia:Riyadh87
Asia:Bangkok	Asia:Kabul	Asia:Riyadh88
Asia:Beirut	Asia:Kamchatka	Asia:Riyadh89
Asia:Bishkek	Asia:Karachi	Asia:Saigon
Asia:Brunei	Asia:Kashgar	Asia:Samarkand
Asia:Calcutta	Asia:Katmandu	Asia:Seoul
Asia:Chungking	Asia:Krasnoyarsk	Asia:Shanghai
Asia:Colombo	Asia:Kuala_Lumpur	Asia:Singapore
Asia:Dacca	Asia:Kuching	Asia:Taipei
Asia:Damascus	Asia:Kuwait	Asia:Tashkent
Asia:Dhaka	Asia:Macao	Asia:Tbilisi
Asia:Dili	Asia:Magadan	Asia:Tehran

continued

Table F-3: Asian Time Zone Settings Supported by the Integrated Administrator
continued

Asia:Tel_Aviv	Asia:Vladivostok	Mideast:Riyadh88
Asia:Thimbu	Asia:Yakutsk	Mideast:Riyadh89
Asia:Thimphu	Asia:Yekaterinburg	PRC
Asia:Tokyo	Asia:Yerevan	ROC
Asia:Ujung_Pandang	Hongkong	ROK
Asia:Ulaanbaatar	Iran	Singapore
Asia:Ulan_Bator	Israel	Turkey
Asia:Urumqi	Japan	
Asia:Vientiane	Mideast:Riyadh87	

Europe

Table F-4 provides the European time zone settings supported by the Integrated Administrator.

Table F-4: European Time Zone Settings Supported by the Integrated Administrator

Eire	Europe:Lisbon	Europe:Skopje
Europe:Amsterdam	Europe:Ljubljana	Europe:Sofia
Europe:Andorra	Europe:London	Europe:Stockholm
Europe:Athens	Europe:Luxembourg	Europe:Tallinn
Europe:Belfast	Europe:Madrid	Europe:Tirane
Europe:Belgrade	Europe:Malta	Europe:Tiraspol
Europe:Berlin	Europe:Minsk	Europe:Uzhgorod
Europe:Bratislava	Europe:Monaco	Europe:Vaduz
Europe:Brussels	Europe:Moscow	Europe:Vatican
Europe:Bucharest	Europe:Nicosia	Europe:Vienna
Europe:Budapest	Europe:Oslo	Europe:Vilnius
Europe:Chisinau	Europe:Paris	Europe:Warsaw
Europe:Copenhagen	Europe:Prague	Europe:Zagreb
Europe:Dublin	Europe:Riga	Europe:Zaporozhye
Europe:Gibraltar	Europe:Rome	Europe:Zurich
Europe:Helsinki	Europe:Samara	GB
Europe:Istanbul	Europe:San_Marino	GB-Eire
Europe:Kaliningrad	Europe:Sarajevo	Poland
Europe:Kiev	Europe:Simferopol	Portugal

Oceania

Table F-5 provides the Oceanic time zone settings supported by the Integrated Administrator.

Table F-5: Oceanic Time Zone Settings Supported by the Integrated Administrator

Atlantic:Azores	Australia:North	Kwajalein
Atlantic:Bermuda	Australia:NSW	NZ
Atlantic:Canary	Australia:Perth	NZ-CHAT
Atlantic:Cape_Verde	Australia:Queensland	Pacific:Apia
Atlantic:Faeroe	Australia:South	Pacific:Auckland
Atlantic:Jan_Mayen	Australia:Sydney	Pacific:Chatham
Atlantic:Madeira	Australia:Tasmania	Pacific:Easter
Atlantic:Reykjavik	Australia:Victoria	Pacific:Efate
Atlantic:South_Georgia	Australia:West	Pacific:Enderbury
Atlantic:St_Helena	Australia:Yancowinna	Pacific:Fakaofo
Atlantic:Stanley	Iceland	Pacific:Fiji
Australia:ACT	Indian:Antananarivo	Pacific:Funafuti
Australia:Adelaide	Indian:Chagos	Pacific:Galapagos
Australia:Brisbane	Indian:Christmas	Pacific:Gambier
Australia:Broken_Hill	Indian:Cocos	Pacific:Guadalcanal
Australia:Canberra	Indian:Comoro	Pacific:Guam
Australia:Darwin	Indian:Kerguelen	Pacific:Honolulu
Australia:Hobart	Indian:Mahe	Pacific:Johnston
Australia:LHI	Indian:Maldives	Pacific:Kiritimati
Australia:Lindeman	Indian:Mauritius	Pacific:Kosrae
Australia:Lord_Howe	Indian:Mayotte	Pacific:Kwajalein
Australia:Melbourne	Indian:Reunion	Pacific:Majuro

continued

Table F-5: Oceanic Time Zone Settings Supported by the Integrated Administrator *continued*

Pacific:Marquesas	Pacific:Pitcairn	Pacific:Tongatapu
Pacific:Midway	Pacific:Ponape	Pacific:Truk
Pacific:Nauru	Pacific:Port_Moresby	Pacific:Wake
Pacific:Niue	Pacific:Rarotonga	Pacific:Wallis
Pacific:Norfolk	Pacific:Saipan	Pacific:Yap
Pacific:Noumea	Pacific:Samoa	US:Hawaii
Pacific:Pago_Pago	Pacific:Tahiti	US:Samoa
Pacific:Palau	Pacific:Tarawa	

Polar

Table F-6 provides the Polar time zone settings supported by the Integrated Administrator.

Table F-6: Polar Time Zone Settings Supported by the Integrated Administrator

Antarctica:Casey	Antarctica:Palmer	Arctic:Longyearbyen
Antarctica:Davis	Antarctica:South_Pole	
Antarctica:DumontDUrville	Antarctica:Syowa	
Antarctica:Mawson	Antarctica:Vostok	
Antarctica:McMurdo		

The Americas

Table F-7 provides the American time zone settings supported by the Integrated Administrator.

Table F-7: American Time Zone Settings Supported by the Integrated Administrator

America:Adak	America:Chihuahua	America:Guatemala
America:Anchorage	America:Cordoba	America:Guayaquil
America:Anguilla	America:Costa_Rica	America:Guyana
America:Antigua	America:Cuiaba	America:Halifax
America:Araguaina	America:Curacao	America:Havana
America:Aruba	America:Dawson	America:Hermosillo
America:Asuncion	America:Dawson_Creek	America:Indiana:Indianapolis
America:Atka	America:Denver	America:Indiana:Knox
America:Barbados	America:Detroit	America:Indiana:Marengo
America:Belem	America:Dominica	America:Indiana:Vevay
America:Belize	America:Edmonton	America:Indianapolis
America:Boa_Vista	America:Eirunepe	America:Inuvik
America:Bogota	America:El_Salvador	America:Iqaluit
America:Boise	America:Ensenada	America:Jamaica
America:Buenos_Aires	America:Fort_Wayne	America:Jujuy
America:Cambridge_Bay	America:Fortaleza	America:Juneau
America:Cancun	America:Glace_Bay	America:Kentucky:Louisville
America:Caracas	America:Godthab	America:Kentucky:Monticello
America:Catamarca	America:Goose_Bay	America:Knox_IN
America:Cayenne	America:Grand_Turk	America:La_Paz

continued

Table F-7: American Time Zone Settings Supported by the Integrated Administrator *continued*

America:Chicago	America:Guadeloupe	America:Los_Angeles
America:Louisville	America:Rainy_River	Brazil:DeNoronha
America:Maceio	America:Rankin_Inlet	Brazil:East
America:Managua	America:Recife	Canada:Central
America:Manaus	America:Regina	Canada:Eastern
America:Martinique	America:Rio_Branco	Canada:East-Saskatchewan
America:Mazatlan	America:Rosario	Canada:Mountain
America:Mendoza	America:Santiago	Canada:Newfoundland
America:Menominee	America:Santo_Domingo	Canada:Pacific
America:Merida	America:Sao_Paulo	Canada:Saskatchewan
America:Mexico_City	America:Scoresbysund	Canada:Yukon
America:Miquelon	America:Shiprock	Chile:Continental
America:Monterrey	America:St_Johns	Chile:EasterIsland
America:Montevideo	America:St_Kitts	Cuba
America:Montreal	America:St_Lucia	Jamaica
America:Montserrat	America:St_Thomas	Mexico:BajaNorte
America:Nassau	America:St_Vincent	Mexico:BajaSur
America:New_York	America:Swift_Current	Mexico:General
America:Nipigon	America:Tegucigalpa	US:Alaska
America:Nome	America:Thule	US:Aleutian
America:Noronha	America:Thunder_Bay	US:Arizona

continued

Table F-7: American Time Zone Settings Supported by the Integrated Administrator *continued*

America:Panama	America:Tijuana	US:Central
America:Pangnirtung	America:Tortola	US:Eastern
America:Paramaribo	America:Vancouver	US:East-Indiana
America:Phoenix	America:Virgin	US:Indiana-Starke
America:Port_of_Spain	America:Whitehorse	US:Michigan
America:Port-au-Prince	America:Winnipeg	US:Mountain
America:Porto_Acre	America:Yakutat	US:Pacific
America:Porto_Velho	America:Yellowknife	
America:Puerto_Rico	Brazil:Acre	

G

Open Source Availability

The Integrated Administrator is based on embedded Linux and contains numerous Open Source components. In compliance with Open Source licensing, HP has made the source code of all Open Source components used available at:

opensource.hp.com

To locate the Integrated Administrator project, consult the list of all projects.

Index

1

128-bit encryption 1-3

A

accessing
  command line interface 4-2
  Integrated Administrator, locally 4-2
  Integrated Administrator, remotely 3-2, 4-2
  server blade RBSU 6-4
ADD
  ADD GROUP command 4-7
  ADD SNMP TRAPRECEIVER command 4-12
  ADD USER command 4-7
  IPMANAGER command 4-35
Add Group screen *See also* Administration tab
  Apply button 3-40
  bay assignment area 3-41
  Cancel button 3-40
  group information area 3-41
  group membership area 3-41
Add User screen *See also* Administration tab
  Apply button 3-37
  Cancel button 3-37
  group membership area 3-39
  user account area 3-38
adding
  existing user to a new group 5-12
  group 5-10
  trap targets 5-28
  user 5-14
administering security certificates 7-4
administration features 1-3
Administration tab *See also* Web-based user interface
  Add Group screen 3-40
  Add User screen 3-37
  Group List screen 3-35
  User List screen 3-33
  View/Modify Group screen 3-42
  View/Modify User screen 3-42
administrator
  changing the password 5-4
  error messages B-5
  warning messages B-3
ADMINISTRATOR
  ASSIGN ADMINISTRATOR RIGHTS command 4-8, 4-11
advanced functions, performing 7-1
African time zone F-3
AlertMail 1-2
  add SMTP server address 5-22
  adding e-mail address, command line 5-22
  disable 5-22
  e-mail header 5-23
  e-mail, adding address 5-22
  enable 5-22

events 5-22
sender domain 5-22
setting up 5-22
severity 5-23
alerts
security 2-7
SNMP 1-2
American time zone F-10
Asian time zone F-4
asset tag number, modifying 5-7
ASSIGN
ASSIGN ADMINISTRATOR RIGHTS command 4-8, 4-11
ASSIGN BAY command 4-8
ASSIGN USER command 4-8
attaching the dianostic adpater 5-19
authorized reseller xiii
Automatic Server Recovery-2 1-6
automatic time configuration
disable 5-25
disable secondary NTP server 5-25
enable 5-25
NTP poll interval 5-25
primary NTP server, set 5-25
secondary NTP server, set 5-25
setting up 5-25

B

BAY
POWEROFF BAY command 4-21
POWERON BAY command 4-21
REBOOT BAY command 4-22
SET BAY UID command 4-23
SHOW BAY INFO command 4-23
SHOW BAY LIST command 4-23
SHOW BAY STATUS command 4-23
SHOW SYSLOG BAY command 4-24
UNASSIGN BAY command 4-24
bay event messages 4-26
Bay Information screen *See also* Bays tab
general area 3-27
status area 3-27
Bay List screen *See also* Bays tab
Action button 3-25
Assign to Group drop-down box 3-25
Bay Assignment button 3-24
Remote Console button 3-24
View Group button 3-24
View/Modify button 3-24
Virtual Buttons button 3-24
BAY LIST, SHOW command 4-35
BAY, ASSIGN command 4-8
BAY, CONNECT command 4-20
Bays tab *See also* Web-based user interface
Bay List screen 3-23, 3-26
Remote Console screen 3-28
Virtual Buttons screen 3-30
BL e-class Integrated Administrator *See* Integrated administrator

C

certificate
Certificate Manager Import Wizard 2-9
Certificate Store 2-9
information window 2-8
security alert 2-7
CERTIFICATE
DOWNLOAD CERTIFICATE command 4-4, 4-28
GENERATE CERTIFICATE command 4-5
C-Gbe Interconnect Switch *See* interconnect switch
changing the administrator password 5-4
CLEAR
CLEAR SCREEN command 4-3
CLEAR SESSION BAY command 4-20, 4-32
CLEAR SESSION SWITCH [A | B] command 4-4
CLEAR SESSION SWITCH command 4-27
CLEAR SYSLOG ENCLOSURE command 4-16

CLEAR BAY BOOT [FIRST | ONCE] command 4-20, 4-33
CLEAR SSHKEY command 4-4, 4-27
command line interface
accessing 4-2
conventions A-1
enclosure management commands 4-16
enclosure network configuration commands 4-12
functionality 4-27
general commands 4-3
general management commands 4-4
guidelines A-1
server bay managment commands 4-20
user account commands 4-7
community string, entering 5-26
components for configuring the diagnostic adapter 5-20
CONFIG, DOWNLOAD command 4-13, 4-31
CONFIG, SHOW command 4-17, 4-31
CONFIG, UPLOAD command 4-20, 4-32
Configuring Server Blade Boot Order 7-7
configuring, SNMP support 5-26
CONNECT
CONNECT BAY command 4-20
CONNECT SWITCH [A | B] command 4-4
connectors
console (serial) 2-3
enclosure link 2-3
locating, illustrated 2-3
management (10/100 Ethernet) connector 2-3
Console Log button 3-24
creating
new group with updated access rights 6-22
security certificates 7-4
customizing enclosure settings 5-4

D

DATE
SET DATE command 4-16
SHOW DATE command 4-18
date, modifying 5-8
deleting
group accounts 6-27
user accounts 6-26
diagnostic adapter
attaching 5-19
components for configuring 5-20
Diagnostics Utility 1-6
DISABLE
ALERTMAIL 4-35
DISABLE SECURESH command 4-12
DISABLE SNMP command 4-12
DISABLE TELNET command 4-12
DISABLE USER command 4-8
DISABLE WEB command 4-12
IPSECURITY command 4-35
NTP command 4-35
disabling and deleting user accounts 6-25
disabling network protocols to the integrated administrator 7-10
DISPLAY EVENT, SHOW command 4-18
DISPLAY EVENTS, SET command 4-5, 4-29
DNS, SET DNS command 4-13
DOWNLOAD
DOWNLOAD CERTIFICATE command 4-4, 4-28
DOWNLOAD CONFIG command 4-13, 4-31
DOWNLOAD SSHKEY command 4-4, 4-28
downloading a security certficate 7-4

E

e-mail, AlertMail 1-2
ENABLE
ALERTMAIL command 4-35
ENABLE SECURESH command 4-13

ENABLE SNMP command 4-13
ENABLE TELNET command 4-13
ENABLE USER command 4-8
ENABLE WEB command 4-13
IPSECURITY command 4-35
NTP command 4-36
enabling remote console sessions to server blades 5-18
enclosure
customizing settings 5-4
error messages B-4
event messages 4-25
factory default settings E-2
generating a summary 6-14
identifying by using the unit identification LED 6-13
identifying problem components 6-16
managing 6-11
modifying the name, 5-5
powering off 7-8
reviewing activity 6-11
system log 6-12
warning messages B-2
ENCLOSURE
CLEAR SYSLOG ENCLOSURE command 4-16
POWEROFF ENCLOSURE command 4-16
SET ENCLOSURE ASSET command 4-17
SET ENCLOSURE NAME command 4-17
SET ENCLOSURE UID command 4-17
SHOW ENCLOSURE FAN command 4-31
SHOW ENCLOSURE INFO command 4-18
SHOW ENCLOSURE POWERSUPPLY command 4-18, 4-32
SHOW ENCLOSURE STATUS command 4-18, 4-32
SHOW ENCLOSURE TEMP command 4-19
SHOW SYSLOG ENCLOSURE command 4-19
ENCLOSURE FAN, SHOW command 4-18
Enclosure Information screen *See also* Enclosure tab
Apply button 3-8
Cancel button 3-8
Date and Time area 3-11
General area 3-9
Integrated Administrator area 3-10
network area 3-10
Power area 3-9
status area 3-8
user-defined time zone window 3-12
Enclosure Self Recovery
features 1-6
Enclosure tab *See also* Web-based user interface
Enclosure Information screen 3-7
Network Configuration screen 3-13
SNMP Configuration screen 3-16
System Log screen 3-21
Virtual Buttons screen 3-19
encryption, 128-bit 1-3
entering a community string 5-26
error messages B-4
administration B-5
enclosure B-4
server blade bay B-4
European time zone F-6
event details D-1
Event List screen *See also* Event List tab
Clear All Events button 3-43
Event List, event descriptions 3-44
View Event Details button 3-43
Event List tab *See also* Web-based user interface
event logging 1-5
event notification
icons D-1
symbols 3-4
EXIT command 4-3

F

factory default settings E-1
enclosure E-2
groups E-3
network E-3
protocol E-3
users E-2
FACTORY, SET command 4-5, 4-29
fan failure
integrated administrator Web-based user interface 6-16
system log 6-18
features
Diagnostics Utility 1-6
Enclosure Self Recovery 1-6
Headless server operation 1-5
Health and Wellness Driver 1-7
HP Management Agents 1-7
Integrated Management Log 1-7
Online ROM flash 1-7
Rapid Deployment Pack (Option) 1-6
Redundant ROM support 1-5
ROM-based Setup Utility 1-5
secure password encryption 1-3
Secure Shell 1-3
Telnet 1-3
flash disaster recovery
automatically launching 7-14
manually launcbing 7-14

G

GATEWAY, SET command 4-14
GENERATE
GENERATE CERTIFICATE command 4-5, 4-28
GENERATE CERTIFICATE SELF-SIGNED 4-5
GENERATE NMI command 4-21, 4-33
generating an enclosure summary 6-14
GROUP
ADD GROUP command 4-7
REMOVE GROUP command 4-8
SET GROUP DESCRIPTION command 4-9
SHOW GROUP command 4-11
Group List screen *See also* Administration tab
Remove Group button 3-36
View/Modify Group button 3-36
group rights to server blade bays, modifying 6-23
group, adding 5-10
grouping feature 1-4

H

Health and Wellness Driver 1-7
health driver 2-2
HELP command 4-3
help resources xii, 2-11
home page 2-10
HP Management Agents 1-7
HP website xiii

I

identifying
a server blade using the unit identification LED 6-9
enclosure by using the unit identification LED 6-13
part number 6-20
problem components 6-16
IMAGE, UPDATE command 4-19, 4-32
IML See Integrated Management Log
Insight Manager 7
compatibility 1-4
server blade configuration 1-6
Integrated Administrator
accessing locally 4-2
accessing remotely 3-2, 4-2
configuration 2-5
default enclosure values E-2
deployment, beginning 2-4
deployment, completing 2-11

description 1-1
disabling network protocols 7-10
error messages B-1
features 1-2
features, administration 1-3
features, AlertMail 1-2
features, automatic network configuration 1-4
features, automatic time configuration 1-4
features, dedicated LAN network connectivity 1-2
features, e-mail alerts 1-2
features, event notification 1-5
features, hyperlinks 1-4
features, remote access and control 1-2
features, security 1-3
features, SNMP 1-2
features, status information 1-5
permission levels 5-3
remote access 3-2, 4-2
summary home page 2-10
troubleshooting C-2
upgrading firmware 7-11
Integrated Administrator configuration, replicating 7-2
Integrated Administrator console, accessing 2-5
Integrated Adminstrator
features, Insight Manager 7 compatibility 1-4
Integrated Management Log 1-7
interconnect switcb
description 1-7
IP address
determining 2-5
enable IP security 5-25
enter 5-25
establishing 2-6
IP security 5-25
remove 5-25
IP security
enable 5-25
setting up 5-24
IPCONFIG, SET command 4-14

K

Key Based SSH Authentication 7-5

L

LAN (Local Area Network)
access 1-2
launching flash disaster recovery 7-13
local access, Integrated Administrator 4-2
Local client device
requirements 2-4
Log In button 2-9
login
screen 3-2
through the command line interface 4-2
Web-based user interface 3-2
Web-based user interface, through the management (10/100 Ethernet) connector 4-2
Web-based user interface, with HTTP 3-2
LOGOUT command 4-3
lost administrator password, recovering 7-12

M

managing
enclosure 6-11
server blade bays 6-2
users 6-22
messages
bay event 4-26
enclosure event 4-25
user event 4-25
modifying
asset tag number 5-7

date 5-8
enclosure name 5-5
group rights to server blade bays 6-23
new group description 5-11
new group name 5-11
new group rights to server blade bays 5-11
rack name 5-5
system contact information 5-28
system location 5-27
time 5-8
user's rights to server blade bays 6-22

N

native graphical remote console 1-3
NETWORK
SHOW NETWORK command 4-15
Network Configuration screen *See also* Enclosure tab
Apply button 3-13
Cancel button 3-13
information area 3-14
Network and Information and Protocols area 3-14
network area 3-14
protocols area 3-14
Network Time Protocol (NTP) 5-25
NIC (Network Interface Card), integrated 1-2
NMI
GENERAGE NMI command 4-33
GENERATE NMI command 4-21
NTP poll interval, set 5-25

O

Oceanic time zone F-7
Online ROM Flash 1-7
opening a remote console session to a server blade 6-2

P

password, administrator 5-4
PASSWORD, SET PASSWORD command 4-9
performing advanced functions 7-1
performing common administrative tasks 6-1
permission levels, ProLiant BL e-Class integrated administrator 5-3
permissions, user 5-3
PING command 4-5, 4-29
Polar time zone F-9
power cycle feature 1-3
powering off
enclosure 7-8
server blade 6-7
POWEROFF
POWEROFF BAY command 4-21
POWEROFF ENCLOSURE command 4-16
POWERON
POWERON BAY command 4-33
POWERON BAY command 4-21
primary NTP server
set 5-25
ProLiant Essentials Rapid Deployment Pack server blade configuration 1-6
protocol, factory default settings E-3

Q

QUIT command 4-3

R

rack name, modifying 5-5
RACK NAME, SET command 4-17
RACK NAME, SHOW command 4-19
RBSU *See* ROM-Based Setup Utility
REBOOT BAY command 4-22, 4-34
reboot, remote 1-3
recovering a lost administrator password 7-12

Redundant ROM support 1-5
remote access 1-2
  Integrated Administrator 3-2, 4-2
Remote Console screen *See also* Bays tab
  Remote Console button 3-28
remote console session, opening to a server blade 6-2
Remote Console, hardware-based 1-3
remote reboot 1-2, 1-3
remote ROM flash 1-7
REMOVE
  IPMANAGER command 4-36
  REMOVE GROUP command 4-8
  REMOVE SNMP TRAPRECEIVER command 4-13
  REMOVE USER command 4-9
removing trap targets 5-29
replicating the Integrated Administrator configuration 7-2
reset and failure sequence replay 1-2
reset sequences, playback 1-2
resetting server, power cycle feature 1-3
RESTART command 4-16
reviewing
  enclosure activity 6-11
  server blade activity 6-6
ROM-Based Setup Utility (RBSU)
  configuration 1-5

S

screen, CLEAR SCREEN command 4-3
SCRIPT MODE, SET command 4-5, 4-30
secondary NTP server
  disable 5-25
  set 5-25
Secure Socket Layer (SSL) 1-3
SECURESH
  DISABLE SECURESH command 4-12
  ENABLE SECURESH command 4-13
security
  alerts 2-7
  features 1-3
security certificates
  administering 7-4
  creating 7-4
  downloading 7-4
server blade
  enabling remote console sessions 5-18
  identifying using the unit identification LED 6-9
  power management options 6-8
  powering off 6-7
  reviewing activity 6-6
server blade bay
  choosing 6-3
  error messages B-4
  modifying group rights 6-23
  warning messages B-3
server blade bay, managing 6-2
server blade health driver See Health and Wellness Driver
server error messages B-1
servers
  startup and shutdown sequence playback 1-2
SESSION BAY
  CLEAR command 4-20
  CLEAR SESSION BAY command 4-32
SESSION SWITCH, CLEAR command 4-27
SESSIONS, SHOW command 4-6, 4-30
SET
  ALERTMAIL command 4-36
  NTP command 4-36
  SET BAY UID command 4-23
  SET DATE command 4-16
  SET DISPLAY EVENTS command 4-5, 4-29
  SET DNS command 4-13
  SET ENCLOSURE ASSET command 4-17

SET ENCLOSURE NAME command 4-17
SET ENCLOSURE UID command 4-17
SET FACTORY command 4-5, 4-29
SET GATEWAY command 4-14
SET GROUP DESCRIPTION command 4-9
SET IPCONFIG command 4-14
SET PASSWORD command 4-9
SET RACK NAME command 4-17
SET SCRIPT MODE command 4-5, 4-30
SET SNMP COMMUNITY command 4-14
SET SNMP CONTACT command 4-14
SET SNMP LOCATION command 4-15
SET USER CONTACT command 4-10
SET USER FULLNAME command 4-10
SET USER PASSWORD command 4-10
SET BAY BOOT FIRST command 4-22, 4-34
SET BAY BOOT ONCE command 4-22, 4-34
SET EXPERT {MODE} [ON | OFF] command 4-5
SET EXPERT {MODE} [ONE | OFF} command 4-29
setting up the system 5-1
setting up user accounts 5-10
settings tag 2-5
SHOW
NETWORK command 4-36
SHOW BAY INFO command 4-23
SHOW BAY LIST command 4-23, 4-35
SHOW BAY STATUS command 4-23
SHOW CONFIG command 4-31
SHOW DATE command 4-18
SHOW DISPLAY EVENT command 4-18
SHOW ENCLOSURE FAN command 4-18, 4-31
SHOW ENCLOSURE INFO command 4-18
SHOW ENCLOSURE POWERSUPPLY command 4-18, 4-32
SHOW ENCLOSURE STATUS command 4-18, 4-32
SHOW ENCLOSURE TEMP command 4-19
SHOW GROUP command 4-11
SHOW NETWORK command 4-15
SHOW RACK NAME command 4-19
SHOW SESSIONS command 4-6, 4-30
SHOW SNMP command 4-15
SHOW SYSLOG BAY command 4-24, 4-35
SHOW SYSLOG ENCLOSURE command 4-19
SHOW USER command 4-11
SHOW CONFIG command 4-17
SHOW EXPERT {MODE} command 4-6, 4-30
SHOW SSHFINGERPRINT command 4-6, 4-30
SHOW SSHKEY command 4-6, 4-30
SHOW TRAY INFO command 4-19
SLEEP <seconds> command 4-3, 4-27
SNMP
ADD SNMP TRAPRECEIVER command 4-12
DISABLE SNMP command 4-12
ENABLE SNMP command 4-13
REMOVE SNMP TRAPRECEIVER command 4-13
SENT SNMP CONTACT command 4-14
SET SNMP COMMUNITY command 4-14
SET SNMP LOCATION command 4-15
SHOW SNMP command 4-15
SNMP Configuration screen *See also* Enclosure tab

Apply button 3-16
Cancel button 3-16
system information area 3-17
SNMP support, configuring 5-26
SSL (Secure Socket Layer) 1-3
startup and shutdown sequence
playback 1-2
status information 1-5
symbols
in text xi
on equipment ix
SYSLOG BAY, SHOW command 4-35
SYSLOG ENCLOSURE, CLEAR
command 4-16
system contact information, modifying 5-28
system features 1-1
system location, modifying 5-27
System Log screen 3-21. *See also*
Enclosure tab
Clear button 3-21
Refresb button 3-21

T

technical support xii
telephone numbers xii, xiii
TELNET
DISABLE TELNET command 4-12
ENABLE TELNET command 4-13
terminal emulation application
opening 2-6
settings 2-6
terminal emulator settings 2-4
time zone settings F-1
Africa F-3
American F-10
Asia F-4
Europe F-6
Oceania F-7
Polar F-9
Universal F-2
time, modifying 5-8
trap targets
adding 5-28
removing 5-29
troubleshooting C-1

U

UNASSIGN
UNASSIGN BAY command 4-24
UNASSIGN USER command 4-11
Universal time zone F-2
UPDATE, UPDATE IMAGE
command 4-19, 4-32
upgrading the integrated administrator
firmware 7-11
UPLOAD
UPLOAD CONFIG command 4-20,
4-32
USER
ADD USER command 4-7
ASSIGN USER command 4-8
DISABLE USER command 4-8
ENABLE USER command 4-8
REMOVE USER command 4-9
SET USER CONTACT command 4-10
SET USER FULLNAME
command 4-10
SET USER PASSWORD
command 4-10
SHOW USER command 4-11
UNASSIGN USER command 4-11
user event messages 4-25
user interface, Web-based 3-3
User List screen *See also* Administration
tab
Remove User button 3-34
View/Modify User button 3-34
users
adding 5-14
disabling and deleting accounts 6-25
factory default settings E-2
managing 6-22

permissions 5-3
setting up accounts 5-10
utilities
Diagnostics Utility 1-6
Enclosure Self Recovery-2 1-6
Insight Manager 7 1-6
ROM-Based Setup Utility 1-5

V

View/Modify Group screen *See also* Administration tab
View/Modify User screen *See also* Administration tab
virtual buttons 7-8
Virtual Buttons screen *See also* Bays tab
Apply button 3-31
enclosure unit identification area 3-19
Power Off button 3-31
Power Off Enclosure button 3-20
Power Off Immediately button 3-31
Reboot button 3-31
Restart Integrated Administrator button 3-20
Toggle On button 3-30
Toggle On/Toggle Off button 3-19
virtual grapbical Remote Console 1-3

W

warning messages B-1
administration B-3
enclosure B-2
server blade bay B-3
WEB
DISABLE command 4-12
ENABLE WEB command 4-13
Web browsers
launching 1-2
Web-based user interface
display areas 3-3
navigating 3-3
panels, deck panel 3-6
panels, left panel 3-5
panels, top panel 3-3
tabs, Administration 3-32
tabs, Administration Add Group screen 3-40
tabs, Administration Add User screen 3-37
tabs, Administration Group List screen 3-35
tabs, Administration User List screen 3-33
tabs, Administration View/Modify Group screen 3-42
tabs, Administration View/Modify User screen 3-42
tabs, Bay Information screen 3-26
tabs, Bay List screen 3-23
tabs, Bay Remote Console screen 3-28
tabs, Bays 3-22
tabs, Enclosure 3-6
tabs, Enclosure Information screen 3-8
tabs, Event List 3-43
tabs, Network Configuration screen 3-13
tabs, SNMP Configuration screen 3-16
tabs, System Log screen 3-21
tabs, Virtual Buttons screen 3-19, 3-30
Web-based user interface, setting up 2-7
websites
HP xiii